



Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para América Latina y Caribe
Registro de Endereços da Internet para América Latina e Caribe

Proyecto AMPARO

Análisis:

Relevancia de la necesidad de una organización de segundo nivel, en la región de América Latina y El Caribe

INDICE

1.- Consideraciones iniciales	pág. 3
2.- Introducción	pág. 4
3.- Breve revisión histórica	pág. 5
4.- Descripción del marco conceptual de las consultas	pág. 7
5.- Datos de base de la encuesta abierta	pág. 7
5.1.- Resumen del análisis de resultados (enc. abierta)	pág. 8
5.2.- Transcripción de comentarios relevantes	pág. 11
5.3.- Resumen de opiniones de encuesta abierta	pág. 12
6.- Resultados de consultas enfocadas	pág. 13
6.1.- Primer consulta enfocada	pág. 13
6.2.- Segunda consulta enfocada	pág. 15
7. Resultados y conclusiones de los relevamientos	pág. 16
8. Anexo I. Resultado de encuesta abierta	pág. 18
8.1.- Anexo I. Resumen de servicios más valorados	pág. 32
8.2.- Anexo I. Resumen de opiniones de gobernabilidad	pág. 43
8.3.- Anexo I. Res. de entrenamiento y capacitación	pág. 52
8.4.- Anexo I. Resumen de tipos de financiamiento	pág. 62
8.5.- Anexo I. Sobre la conformación equipo técnico	pág. 70
8.6.- Anexo I. Comentarios finales de la encuesta	pág. 72
9.- Bibliografía	



Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para América Latina y Caribe
Registro de Endereços da Internet para América Latina e Caribe

1.- Consideraciones iniciales

El presente análisis ha sido desarrollado en el marco de las actividades del Proyecto AMPARO, una iniciativa de LACNIC con el apoyo de IDRC de Canadá.

El equipo que ha estado trabajando en el desarrollo del mismo desea agradecer la colaboración de muchas personas de la región de América Latina y el Caribe que han donado generosamente su tiempo contestando nuestras (interminables) preguntas.

Hemos intentando que los resultados obtenidos, puedan reflejar las opiniones más aceptadas de la región respecto de la necesidad de la existencia de una organización de segundo nivel que propenda a una estandarización y mejor coordinación acerca de la Gestión de Incidentes de Seguridad Informática, y esperamos que sea de utilidad para todos aquellos que tenemos el cometido y la vocación de promover el desarrollo de una Internet confiable, útil para los ciudadanos, y que permita mejorar la calidad de vida de nuestros países.

Es nuestro deseo que el presente documento fomente la discusión y genere nuevos espacios de colaboración y mejora, entre los equipos y organizaciones de seguridad de la región.

De nuevo, gracias...

Mag. Ing. Edgar Vega Briceño

Consultor

Ing. Vinicio Vasquez

Consultor

Msc. Ing. Eduardo Carozo Blusmztein, CIS

Coordinador del Proyecto AMPARO

CONTENIDOS

2. Introducción

Nuestra región, América Latina y el Caribe, está obteniendo crecimientos en el acceso a Internet del orden del 20% anual, llegando a 212 millones de personas en marzo de 2011¹. Se espera que dicho crecimiento se mantenga en el futuro debido a la inclusión de nuevas tecnologías que provocan menores dificultades para el ciudadano, tanto en términos de costos, como en términos de facilidad de utilización.

Las empresas y gobiernos de la región están proveyendo servicios cada vez más novedosos y haciendo más independientes a las personas de las locaciones físicas para resolver necesidades de todo tipo (financieras, servicios, etc.).

Dada la expansión de dichos servicios, obviamente existen incidentes de seguridad informática que afectan la disponibilidad y confiabilidad de los servicios brindados a través de la Internet. La región atendida por LACNIC comprende a 33 países y hasta el momento en la misma han sido acreditados en el FIRST, sólo 11 equipos, distribuidos en 7 países². En un relevamiento manual realizado por los autores del presente documento, se han detectado al menos 30 equipos que se dedican full time a la actividad de gestionar incidentes de seguridad informática, en la región.

En este contexto se ha identificado la necesidad de analizar la pertinencia sobre el desarrollo de una organización que brinde soporte de capacitación, coordinación y gestión a Centros de Respuesta a Incidentes de Seguridad Informática de América Latina y el Caribe.

En el Proyecto AMPARO, hemos realizado múltiples encuestas y consultas de opinión, algunas masivas, a personas que están en contacto con incidentes de seguridad informática y otras enfocadas, a través de entrevistas personales y/o focus-group, a personas de reconocida experiencia en la disciplina radicadas en la región.

Es justo destacar la alta colaboración y paciencia de nuestros colegas, que han descuidado (por nuestras consultas!!) algunos minutos de sus agitadas agendas, haciendo honor de su compromiso con la colaboración en seguridad, actividad trascendente para mejorar la eficacia y eficiencia de nuestros equipos,... a ellos vaya un gran agradecimiento de éste equipo de trabajo.

¹ Según internet worldstats

² Según www.first.org

3.- Breve revisión histórica

El Proyecto AMPARO, nace en Junio de 2009 como una iniciativa de LACNIC que junto con IDRC, deciden financiar la creación y difusión de contenido académico especialmente adaptado a la realidad de América Latina y el Caribe en todo lo concerniente a la gestión de incidentes de seguridad informática.

Se han cumplido hasta el momento todas las metas y objetivos propuestos, en muchos casos con cumplimientos que casi duplicaron lo planificado. Ejemplos de esta situación es que se han realizado 7 talleres en diferentes países, se han entrenado alrededor de 300 técnicos, se ha aprobado al menos a 8 entidades universitarias o gubernamentales a utilizar el contenido creado para su posterior replicación, se han realizado al menos cuatro documentos de amplia difusión en la comunidad y se ha popularizado el Manual de Gestión de Incidentes de Seguridad Informática, al grado que existen por lo menos 20 sitios de Seguridad Informática que lo han “linkeado” como material de referencia.

Simultáneamente se han financiado proyectos de investigación en seguridad informática, en cinco universidades de la región, que están prontos a ser culminados y que generarán más y mejor contenido para la comunidad.

Se están apoyando en este corto período, 6 iniciativas de creación de CSIRT's de diferentes organizaciones en Ecuador, El Salvador, Colombia y México.

Sin embargo, lo que consideramos más relevante de la actividad ha sido la interacción y relacionamiento posterior que entre los participantes del Taller AMPARO se instala, al grado que buena parte de los mismos están integrados a un grupo en Facebook denominado “Proyecto AMPARO”, que en este momento tiene alrededor de 240 miembros, muchos de los cuales colaboran y generan alertas y comunicados para el resto.

Frente a esta realidad se ha decidido llevar adelante éste análisis, como parte del reconocimiento de las virtudes y carencias que en nuestro entorno regional existen, basado en consultas participativas hacia los integrantes de estos grupos de interés y actividad. También se han realizado consultas enfocadas a especialistas reconocidos de la región, así como entrevistas a un reducido conjunto de expertos.

Antecedentes históricos relevantes

El precursor de las organizaciones de segundo nivel ha sido el **CERT/CC**. Dicho centro surge como respuesta del Gobierno de los Estados Unidos frente a un incidente denominado “gusano de Morris” ocurrido en los albores de la red de redes (año 1988), que dejó una muy clara evidencia de la alta vulnerabilidad que generaba la existencia de una gran red interconectada de procesadores, principalmente por la baja preparación de los centros que la integraban, para actuar de forma coordinada ante una emergencia.



Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para América Latina y Caribe
Registro de Endereços da Internet para América Latina e Caribe

Dicho centro hospedado en la Carnegie Mellon University, ha desarrollado contenidos que son referencia mundial en la disciplina y dada la alta cantidad de centros en Norteamérica (alrededor de 80 equipos registrados en FIRST), se ha convertido por la vía de los hechos en un Centro de Segundo Nivel para dicha región y es un caso de éxito de alcance global.

Actualmente la región europea cuenta con cerca de 80 equipos registrados en FIRST. Existieron varios intentos para la creación de un CERT regional en el año 1997, (en esa época se disponía de 28 equipos de seguridad en dicha región), denominado EuroCERT, que fracasa debido al bajo apoyo inter-institucional recibido. Posteriormente en el año 2004 se crea la Agencia Europea de la Seguridad de las Redes y de la Información **ENISA** creada por la Unión Europea, para prevenir y responder a los problemas de seguridad de la información de los países miembros. Actualmente está consolidando su posicionamiento y liderazgo con variadas propuestas de entrenamiento y realización de eventos y reuniones.

En tanto en la región de Asia Pacífico, en el año 2003, se ha creado **APCERT** promovido por 15 CERTs/CSIRTs de la región. Actualmente dispone de dos tipos de membresías General Members y Full Members. Entre ambas categorías actualmente 27 equipos están afiliados a sus membresías. Brinda servicios de intercambio de información, actualización y realiza eventos regionales de entrenamiento y actualización en seguridad.

Finalmente existe un foro global (Forum of Incident Response Security Teams) **FIRST**, que brinda servicios de intercambio de información, actualización y realiza eventos mundiales y regionales de entrenamiento y actualización. Dicho foro reúne 220 centros de todo el mundo y utiliza exclusivamente el idioma inglés. Los equipos se vinculan a través de un proceso de revisión realizado por dos miembros del Foro, y el pago de una membresía anual. Existen también equipos de trabajo para temas específicos.

En tanto en la región existen algunas iniciativas que han comenzando a generar espacios de colaboración y cooperación, como ser el propio **Proyecto AMPARO**, **LACSEC** y las **Listas de Seguridad de LACNIC**, dentro de la importante esfera de influencia de LACNIC, así como actividades de concientización y capacitación llevadas a cabo por el **CICTE** (Comité Interamericano contra el Terrorismo) **de la OEA** que han estado en general enfocadas en coordinar entidades vinculadas a los gobiernos de las Américas.

4.- Descripción del marco conceptual de las consultas

Con esta iniciativa se ha pretendido relevar las opiniones de los actores principales de la comunidad de Internet de América Latina y el Caribe buscando una opinión de consenso respecto de la pertinencia y la necesidad de disponer de una organización que vincule a los mismos para resolver en forma más eficiente los desafíos que se están presentando por temas de seguridad en Internet a nivel regional y mundial.

Por otro lado, el presente estudio intenta reflejar la opinión de un colectivo especializado, sin asumir como propuesta una solución estándar aplicada en otras regiones.

Marco metodológico

Para la realización de la tarea se han llevado a cabo tres actividades principales como mecanismo de flujo de la información para luego ser analizada y difundida. Se atendió, en primera instancia, una **encuesta abierta** a toda la comunidad de expertos en seguridad informática la cual ha sido contestada en forma anónima por 124 personas en la cual se han realizado 54 preguntas las cuáles han sido agrupadas en los siguientes metaconceptos:

- Tipos de servicios.
- Gobernabilidad y ejecución.
- Entrenamiento y capacitación.
- Financiamiento
- Equipo técnico.

Luego se realizó una segunda actividad la cual constituyó una **consulta enfocada** a 20 actores identificados como directores o gerentes técnicos de Centros de Respuestas de la región con un nivel de “expertise” más alto de los temas relacionados. Estas preguntas han sido realizadas sobre una lógica más abierta, la consulta no fue de carácter anónimo. Finalmente se recabaron **opiniones en forma directa** de actores claves, que han expresado opiniones que serán consideradas a continuación.

Todas las respuestas en el presente informe, serán manejadas en forma estadística, sin identificar a las personas que han respondido.

5.- Datos de base de la Encuesta abierta.

Se consultaron alrededor de 800 personas identificados como usuarios intensivos de Tecnologías de la Información, con interés expresado en Seguridad Informática, a través de dos medios de comunicación: 1.- Las listas de seguridad de LACNIC y 2.- Los contactos establecidos por los participantes del Proyecto AMPARO.

De dicho universo se obtuvieron alrededor de 150 respuestas totales y 124 respuestas completas y coherentes. Las 26 respuestas no contabilizadas fueron analizadas y se descartaron por no estar completamente respondidas, no se detectó ningún caso de respuestas malintencionadas o contestadas en forma incoherente.

5.1.- Resumen del análisis de resultados

Sobre Tipos de servicios a brindar por la organización

Se detallan a continuación aquellos servicios que han sido valorados con más de un 80%, en los tópicos extremada/alta relevancia.

SERVICIO	VALORACIÓN
Divulgación de Información relacionada con Seguridad	92%
Coordinación para la respuesta a incidentes de seguridad	90%
Capacitación a otros Centros de Respuesta	90%
Educación, concientización de la Comunidad	88%
Realización de Eventos Internacionales de Seguridad	87%
Alertas y advertencias	82%

Como se observa en base a los resultados que contestaron: “extremadamente relevante” o “alta relevancia”, los servicios de coordinación, difusión y entrenamiento han sido identificados como los más oportunos para el momento que la región está viviendo.

Sobre Gobernabilidad y Ejecución de la organización a formar

Se consultó específicamente cuál sería el sistema de gobernabilidad que mejor representaría los intereses de la comunidad, en caso de existir un foro u organización de segundo nivel. Se obtuvieron las siguientes respuestas:

SERVICIO	VALORACIÓN
Directorio por un representante de cada CSIRT/CERT	69%
Directorio por personas destacadas de la región	69%
Directorio por un representante de cada país	63%
Directorio Académico	42%
Directorio elegido por asamblea representativa	36%

Se observa que la representación elegida es basada en la confianza de personas físicas reconocidas por la comunidad, asociadas a instituciones (de seguridad reconocidas por ejemplo CERT.br, académicas por ejemplo UNAM-CERT o gobiernos por ejemplo ARCert).

Sobre Entrenamiento y Capacitación necesarios en la región

Se detallan a continuación los resultados de las consultas

TIPO DE ENTRENAMIENTO	VALORACIÓN
Resolución de incidentes en tiempo real (botnet)	90%
Acceso a repositorio de lecciones aprendidas	90%
Formación y gestión de Centros de Respuesta	87%
Resolución de incidentes en tiempo real (phishing)	84%
Realizar un evento anual de seguridad para la región	83%
Resolución de incidentes en tiempo real (honeynet)	82%
Gerenciamiento de Centros de Respuesta	81%
Uso de herramientas forenses	80%

Se han contestado todas las propuestas de capacitación y entrenamiento con un 80% o más, demostrando la relevancia de las actividades desarrolladas hasta el momento por el Proyecto AMPARO. La relevancia más alta se ha evidenciado en resolución de incidentes y el entrenamiento para la formación de equipos de respuesta, incluida la necesidad de proveer un centro de lecciones aprendidas sobre incidentes y su resolución.

Sobre Financiamiento de las actividades de la organización a formar

Se detallan a continuación los resultados de las consultas

TIPO DE FINANCIAMIENTO	VALORACIÓN
Cobros por entrenamiento y capacitación	73%
Cobros por consultoría	67%
Cobros por certificaciones de SGSIs	65%
Presupuesto por organización host	65%
Cobro de membresía anual a organizaciones	63%

Como se desprende de las respuestas el proceso de financiamiento se espera sea basado en cobros por cupos en entrenamiento y capacitación, consultoría y a través de presupuestos otorgados por la organización que aloja el Foro o Centro de Coordinación.

También se considera relevante por parte de los respondentes, el cobro de posibles acreditaciones de Sistemas de Gestión de Seguridad de la Información, y la posibilidad de cobrar membresías anuales a grandes organizaciones, a cambio de integrarse al foro.

Sobre la conformación del Equipo Técnico

Se detallan a continuación los resultados de las consultas

CONFORMACIÓN EQUIPO TÉCNICO	VALORACIÓN
Necesidad de coordinador técnico full time	86%
Los técnicos pueden estar alocados en diferentes países	80%
Debe existir un código de ética y acuerdos de confidencialidad, expresamente aceptados x los técnicos	95%
Disponer de una red de comunicaciones segura	92%

Se concluye entonces que la comunidad entiende necesaria la existencia de un coordinador técnico de carácter full-time, con un equipo técnico posiblemente distribuido en los países atendidos y con una infraestructura de comunicaciones segura. Se entiende también altamente necesario que el equipo debe confirmar su adhesión a un código de ética y a unas estrictas políticas de seguridad de la información, que exijan su compromiso con la firma de acuerdos de confidencialidad adecuados.

5.2.- Transcripción de comentarios relevantes

A continuación se transcriben algunos comentarios literales que se respondieron en la pregunta “abierta” a tales efectos:

1- *“Se entiende extremadamente importante la realización de eventos de difusión de las mejores prácticas, técnicas utilizadas por las personas que actúan en forma maliciosa y promover una red de técnicos que ayude a la rápida respuesta de los incidentes a nivel internacional.”*

2- *“Un CSIRT coordinador regional es muy importante en la actual época debido a los distintos ataques e incidentes de seguridad, en este caso los CSIRT nacionales deberían de estar previamente establecidos para mantener una comunicación y apoyo fluido.”*

3- *“Pienso que se debe considerar el tema de la vinculación de la Educación en temas de seguridad, que haya una parte para la Investigación científica en temas de seguridad informática...”*

...

7- *“Dar más divulgación sobre estos temas y tener un representante para que esto se haga más extensivo a nivel no solo público sino privado.”*

8- *“The most important question to be asked was: is there a need to a CSIRT for the region? I think there is a need for a forum for CSIRTs, but not for a coordinating CSIRT. I don't see a point in us repeating the errors of Europe when they tried to create the "EuroCERT" back in the 90's...//... there are no questions that give an option of forming a structure similar to TF-CSIRT or APCERT -- they are not operational, they are a coalition of CSIRTs that work towards cooperation.”...*

...

10- *“Me parece importante considerar la inclusión de esta figura de la coordinación de certs en algún organismo que pueda darle presupuesto anual y que garantice su funcionamiento en el tiempo.”*

11- *“Se puede pensar en una especie de asociación de CSIRTs de la región, como un FIRST latinoamericano, que sea fuente de difusión de información, apoye la operación y*

creación de CSIRTs en la región comprendiendo nuestra realidad y que se lo "sienta" más cercano. ..."

12- "La eventual organización que coordine a los Centros de Respuesta a Incidentes de Seguridad Informática de América Latina y el Caribe, debería ser independiente de toda otra organización regional existente. ..."

5.3.- Resumen de opiniones de la Encuesta Abierta

Como se puede observar las opiniones expresan la necesidad de un proceso de creación desde las organizaciones existentes (CERT, Csirt, o Equipos de Respuesta) en base a una asociación o foro de dichos equipos, que promueva la formación de redes de confianza, intercambio de capacidades y realización de entrenamientos reuniones.

Los servicios relevantes que dicha organización debería brindar deberían ser: Divulgación de Información relacionada con seguridad, Coordinación para la respuesta a incidentes de seguridad, Capacitación a otros Centros de Respuesta, Entrenamientos y concientización de la Comunidad, Realización de Eventos Internacionales de Seguridad y Alertas y Advertencias.

Dicho centro debería disponer de un Steering Committee, que tenga representación de los CSIRT's que lo conforman, así como una mínima estructura de soporte, basada en un coordinador técnico actuando en régimen full-time, y algunos técnicos radicados en diferentes países, actuando posiblemente en régimen part-time.

Los entrenamientos considerados más relevantes son aquellos vinculados a los ataques de mayor impacto (botnet y phishing) y de alta frecuencia en la región, así como la asistencia a la creación de centros de respuesta.

Se entiende que los fondos de conformación y operación del mencionado centro deberían provenir de Cobros a cambio de entrenamientos y capacitación, consultoría y la consecución de un presupuesto por parte de la organización que alojaría dicho foro.

Por más información, puede ver los resultados completos de la encuesta abierta en el ANEXO I, del presente documento.

6.- Resultados de consultas enfocadas

6.1.- Primer Consulta Enfocada:

Consideraciones iniciales:

Se realizó y envió un documento de consulta, a 27 líderes de equipos de seguridad de países de la región, que iniciaba identificando al respondente, con una serie de preguntas que se detallan a continuación, obteniéndose 12 respuestas.

Están representadas en ésta muestra las industrias: Telecomunicaciones, Banca, Gobierno, Academia, y un Proveedor de Hardware de clase mundial.

A continuación se tratarán las respuestas en forma individual:

Pregunta 1: *¿Considera relevante para la consecución de resultados exitosos que, mientras labora en el control y mitigación de incidentes de seguridad informática, exista algún grado de coordinación entre las organizaciones afectadas?*

Todas las respuestas se centraron en identificar este aspecto como **fundamental, imprescindible, ...única forma**, de resolver en forma exitosa las tareas de control y mitigación de incidentes de seguridad.

Pregunta 2: *¿Considera que la coordinación e intercambio que usted recibe en la resolución de los incidentes de seguridad informática es suficiente?*

Esta pregunta ha sido contestada por la negativa en 7 oportunidades (dichas respuestas fundamentalmente fueron dadas por responsables de telecomunicaciones y academia) y afirmativamente por 5 consultados (personas del sector gobierno y banca)

Pregunta 3: *¿Las fuentes de información, deberían ser validadas por algún actor regional reconocido por la comunidad? ¿Cuál sería el mecanismo más apropiado para validar la información recibida?*

Se contestó en 9 oportunidades que era necesaria la existencia de algún organismo regional que validara la información, a través de una base de datos con firma digital y hospedada por algún actor de reconocido prestigio, 2 respuestas consignaron que ya existen actores regionales de reconocido prestigio que podrían prestar estos servicios.

Pregunta 4: Valore por favor sustituyendo la X por la valoración numérica sugerida más abajo, la importancia para usted de la información a compartir:
 (1-irrelevante; 2-poco importante; 3-interesante; 4-importante; 5-crucial)

Información a compartir	Factor promedio – respuestas
Información sobre incidentes ocurridos	4,5,4,3,5,4,2,4,5,5,5,4 – 4.17
Información sobre incidentes ocurriendo en tiempo real	3,5,4,4,5,5,5,5,5,5,4 – 4.58
Información sobre vulnerabilidades	5,4,3,5,4,4,2,5,4,4,4,4 – 4.00
Información sobre posibles motivadores de ataques	4,4,5,5,4,4,4,4,4,4,5 – 4.25
Información sobre técnicas de mitigación de incidentes	4,5,4,5,4,3,3,4,5,5,4,5 – 4.25

Pregunta 5: *¿Cuáles serían, a su criterio, los mecanismos para lograr una coordinación más adecuada?*

Generar redes de confianza o similares (es decir organizaciones ad-hoc con autoridad conseguida en base a legitimidad), ha sido respondida en 7 ocasiones, en un par de respuestas se visualiza al Proyecto AMPARO realizando esta función en la actualidad.

La creación de un **Centro de Seguridad Coordinador o similar** (es decir una organización con autoridad formal, delegada por los demás Csirt o CERT) ha sido propuesta en cinco respuestas.

Pregunta 6: *Además de compartir información sobre incidentes, ¿Qué apoyos o servicios adicionales requiere para desempeñar efectivamente su actividad laboral?*

1. Apoyo y complementaciones técnicas entre las organizaciones, intercambio de información.
2. Uniformización de procedimientos entre los grupos de gestión de incidentes, regulados por un ente común y confiable.
3. Mucho entrenamiento y constante actualización.
4. La generación de materiales para actualización de conocimientos y entrenamientos
5. Poder compartir espacios que auspicien el intercambio de know-how, una interconexión dinámica entre actores, tanto en lo académico, como en lo profesional.

Pregunta 7: Observaciones y sugerencias:

- 1.- En América Latina el creciente uso de internet cada año ha sido más significativo que el anterior, por ese motivo creo que se debería trabajar más focalizado en instituciones de gobierno y privadas de los países para que los eventos de seguridad no nos afecten tanto.
- 2.- Remarcar que considero de alta relevancia estratégica en relación al desarrollo social y productivo de nuestros países contar con centros de coordinación para la gestión de incidentes de seguridad con elevada capacidad operativa y funcional.
- 3.- Es importante trabajar en la difusión de logros y avances del proyecto con otros organismos, en virtud de no mezclar el carácter del grupo con otros esfuerzos, como por ejemplo la OEA; por el contrario, aprovechar para sumarnos en actividades comunes, dado que varios de los actores somos los mismos en distintos foros; sin embargo el esfuerzo de AMPARO es incluyente y no solo de carácter gubernamental.
- 4.- Sería bueno que se realicen visitas a nivel regional y que se expongan a través de charlas la importancia de crear ésta organización regional
- 5.- Varias respuestas agradecieron la oportunidad de poder expresar sus opiniones y felicitaron la iniciativa.

6.2.- Segunda Consulta Enfocada:

En Abril de 2011, se realiza en Montevideo la reunión anual del Steering Committe del Proyecto AMPARO, con varios invitados relevantes de la comunidad de seguridad informática de la región.

En consecuencia se dedicaron algunas horas de dicha reunión a discutir y buscar respuestas más consistentes a algunas de las preguntas que generaron dudas, ya sea por el hecho de que la comunidad no diera una respuesta única, ya sea porque la pregunta podría dar lugar a más de una interpretación por parte de la persona consultada.

Dicha reunión ha arrojado las siguientes opiniones, después del análisis pormenorizado de la información, hasta ahora tratada:

- 1.- Es claramente detectada la necesidad de la existencia de una organización que brinde la capacitación y entrenamiento ya mencionadas, así como se detectan claros espacios de acción para crear los mecanismos necesarios para mejorar la insuficiente coordinación actual.
- 2.- Que la formación de dicha organización debe ser iniciativa de un grupo de Cert/Csirt de la región que lidere el proceso de adhesión de los demás centros a la iniciativa.

3.- Que es necesario generar lo antes posible una red de confianza, a través de reuniones regionales convocando a los Centros de Respuesta de la región, así como generar una serie de exposiciones para concientizar a los “hacedores de políticas nacionales y regionales”

7. Resultados y conclusiones de los relevamientos.

- Dados los incidentes de alto impacto que están ocurriendo hoy en día y la recepción de información obtenida, se entiende necesario **seguir con el proceso iniciado de aumentar las capacidades de respuesta de la región a los incidentes de seguridad informática y de la información** mediante entrenamientos especializados y creación de contenidos académicos actualizados y pertinentes para la región.
- Se ha identificado **como principal dificultad, la falta de capacitación actualizada y sistemática para enfrentar estas problemáticas**, tanto a nivel del usuario, como de los técnicos involucrados con el mantenimiento de los servicios.
- También se ha identificado, como una **dificultad muy importante** la falta de puntos de escalamiento de incidentes, coordinación y respuesta estándar a los incidentes de seguridad de la información debido a **la falta o desconocimiento de la existencia de Centros de respuesta a incidentes de seguridad organizacionales y/o nacionales**.
- Se ha identificado como un **problema relevante la falta de una organización que establezca un segundo nivel de confianza**, simplificando las múltiples comunicaciones punto a punto que se establecen en un incidente masivo de seguridad informática.
- Se ha identificado que **la forma más aceptada de constituir ésta organización, es desarrollar un foro de seguridad regional** que provea estandarización y comunicaciones seguras entre los centros que lo auspicien y viabilicen.
- Se recomienda para el fomento del nacimiento de dicha organización de segundo nivel, la **realización de encuentros regionales periódicos** entre personal encargado de la gestión de los centros de respuesta existentes, que tengan como objetivo compartir experiencias, proveer actualización técnica y promover el aumento de confianza de las relaciones entre los técnicos y Centros de Respuesta.
- **Se recomienda** realizar éstas actividades con **un adecuado plan de comunicación y coordinación con las múltiples organizaciones** que están operando en la región de manera de maximizar el impacto del esfuerzo invertido.

Fin de documento principal.



Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para **América Latina y Caribe**
Registro de Endereços da Internet para **América Latina e Caribe**

Página dejada en blanco intencionalmente.

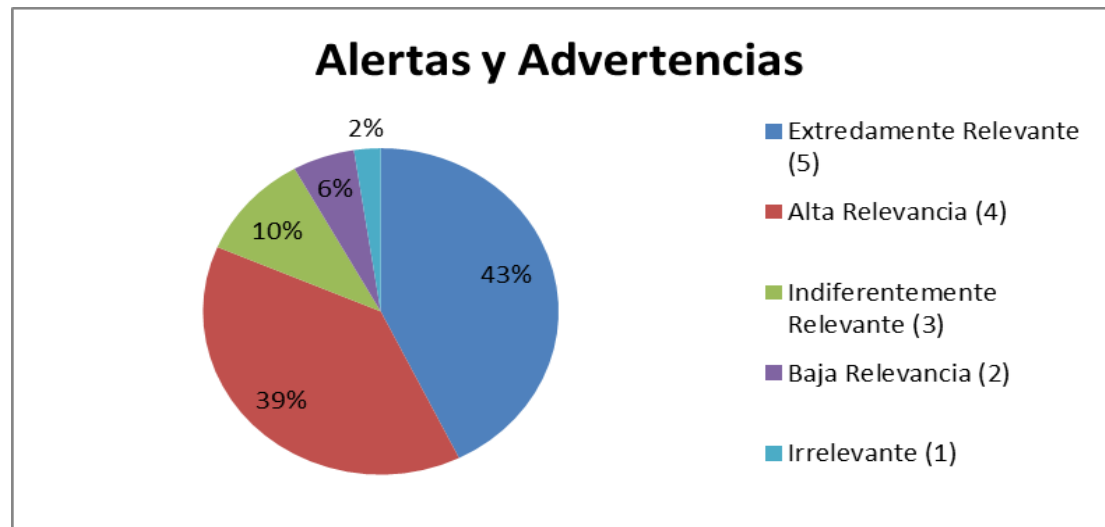
ANEXO I: RESULTADOS de ENCUESTA ABIERTA

“TIPOS DE SERVICIOS”

Alertas y Advertencias

Responde a: Relevancia de contar con servicios de alertas y advertencias en un eventual organismo de coordinación regional.

Resultados:



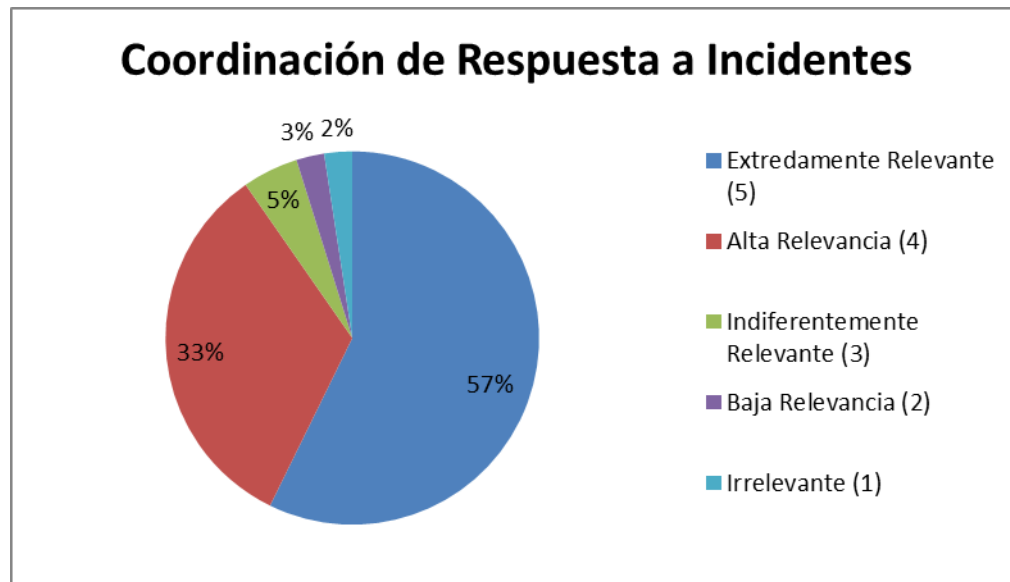
Fuente: Encuesta en línea de elaboración propia. Anexo N°1.

Por lo anterior, la población encuestada considera que es indispensable contar con el servicio de alertas y advertencias dentro del catálogo de servicios en un Centro de segundo nivel, al tener **82% de relevancia** para los expertos de la región según la opinión de la muestra.

Sobre Tipos de Servicios

Responde a: Relevancia o no relevancia de contar con servicios de coordinación de respuestas a incidentes en un organismo de coordinación regional.

Resultados:



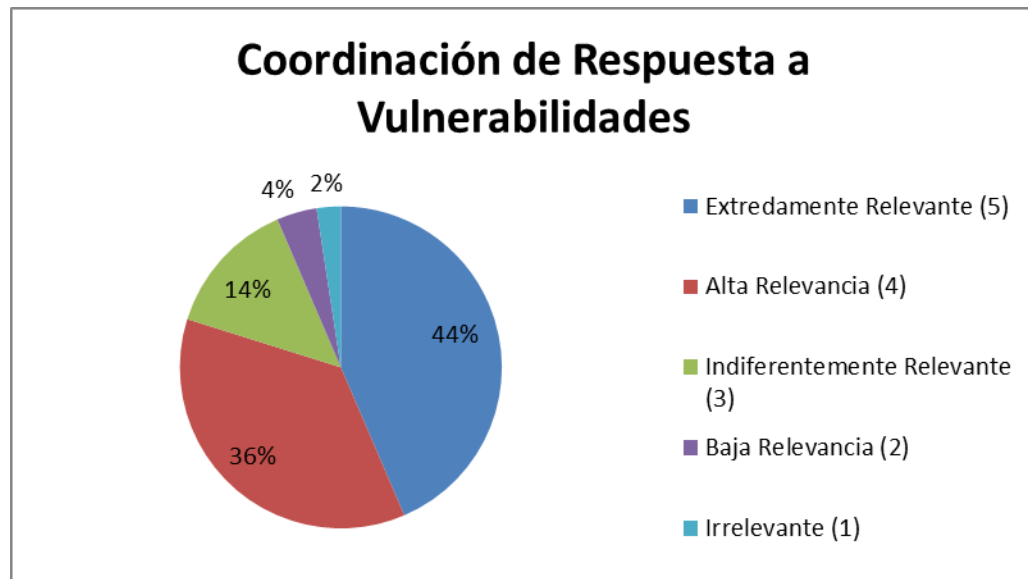
Fuente: Encuesta en línea de elaboración propia. Anexo N°1.

Por lo anterior, la población encuestada considera entonces que es indispensable contar con la **coordinación de respuestas a incidentes** dentro del catálogo de servicios en un organismo de coordinación regional, al tener **90% de relevancia** para los expertos de la región según la opinión de la muestra.

Sobre Coordinación de Respuesta a Vulnerabilidades

Responde a: Relevancia o no relevancia de contar con servicios de coordinación de respuestas a vulnerabilidades en un organismo de coordinación regional.

Resultados:



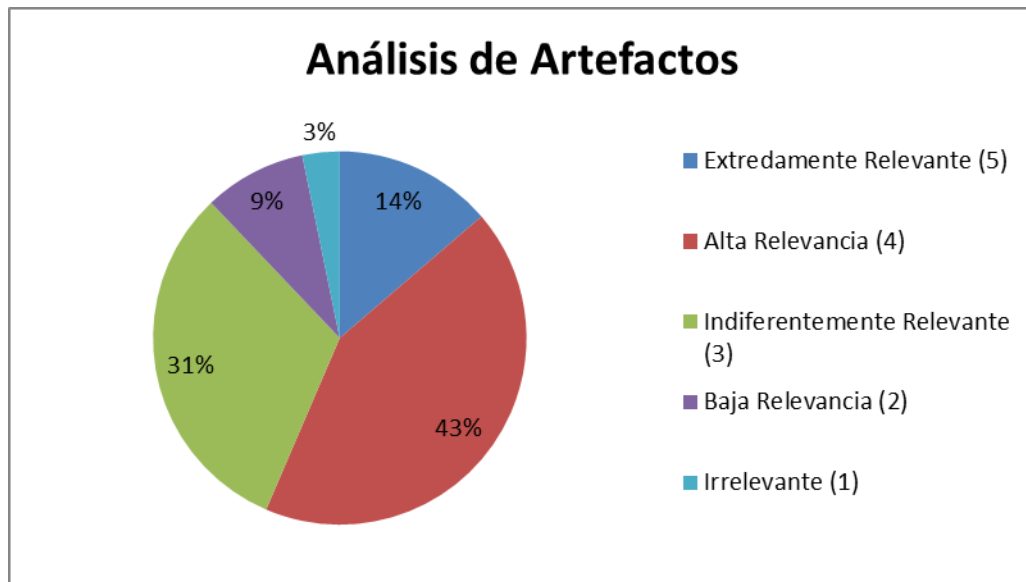
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera que es recomendable contar con la coordinación de respuestas a vulnerabilidades dentro del catálogo de servicios en un organismo de coordinación regional, al tener **80% de relevancia** para los expertos de la región según la opinión de la muestra.

Sobre Análisis de Artefactos

Responde a: Relevancia o no relevancia de contar con servicios de análisis de artefactos en un eventual organismo de coordinación regional.

Resultados:



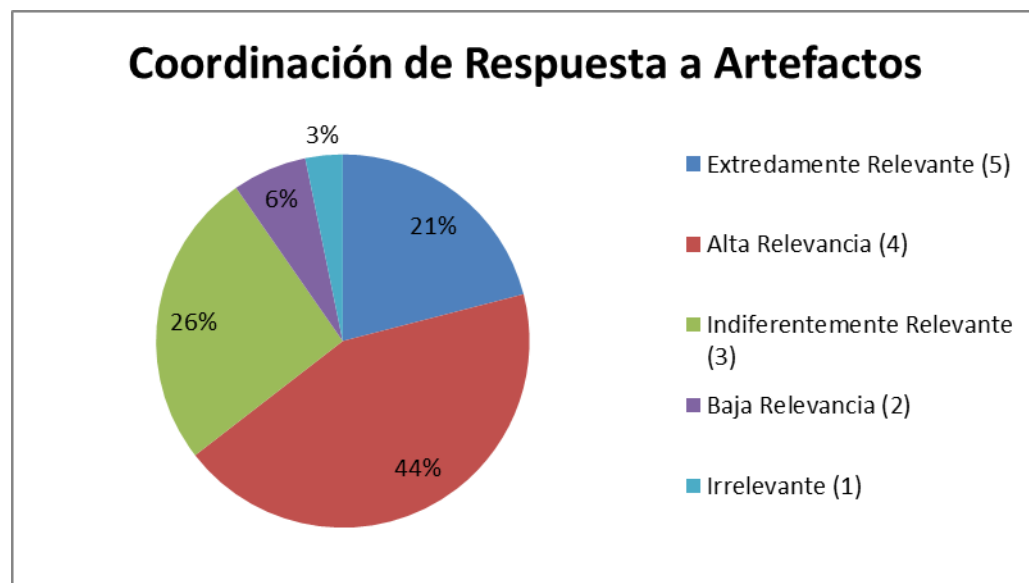
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera entonces conveniente contar con el análisis de artefactos dentro del catálogo de servicios en un organismo de coordinación regional, al tener **57% de relevancia** para los expertos de la región según la opinión de la muestra.

Sobre Coordinación de Respuesta a Artefactos

Responde a: Relevancia o no relevancia de contar con servicios de Coordinación de Respuesta a Artefactos en un eventual organismo de coordinación regional.

Resultados:



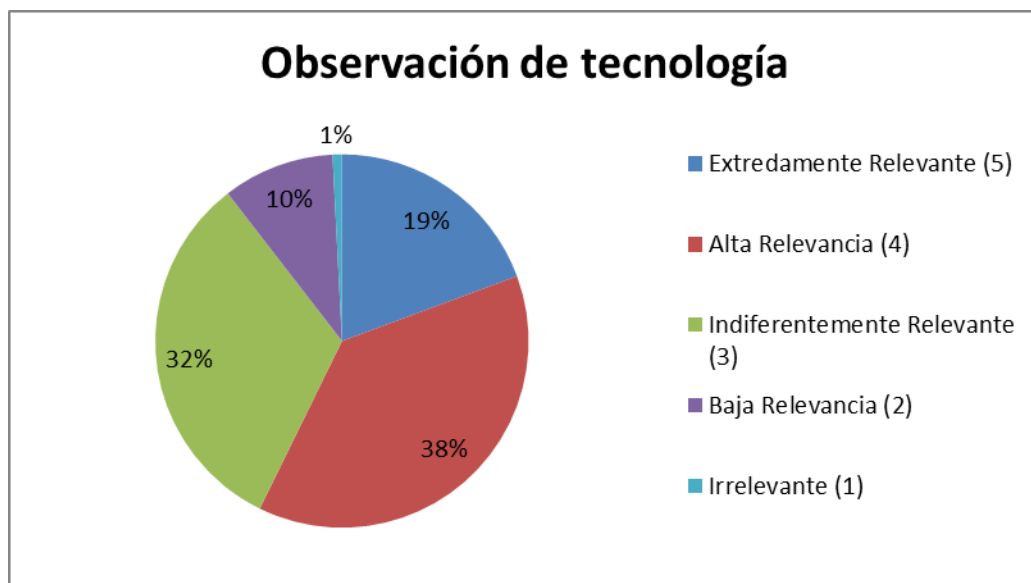
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera entonces conveniente contar con la coordinación de respuesta a artefactos dentro del catálogo de servicios en un organismo de coordinación regional, al tener 57% de relevancia para los expertos de la región según la opinión de la muestra.

Sobre Observación de Tecnología

Responde a: Relevancia o no relevancia de contar con servicios de Coordinación de Respuesta a Artefactos en un eventual organismo de coordinación regional.

Resultados:



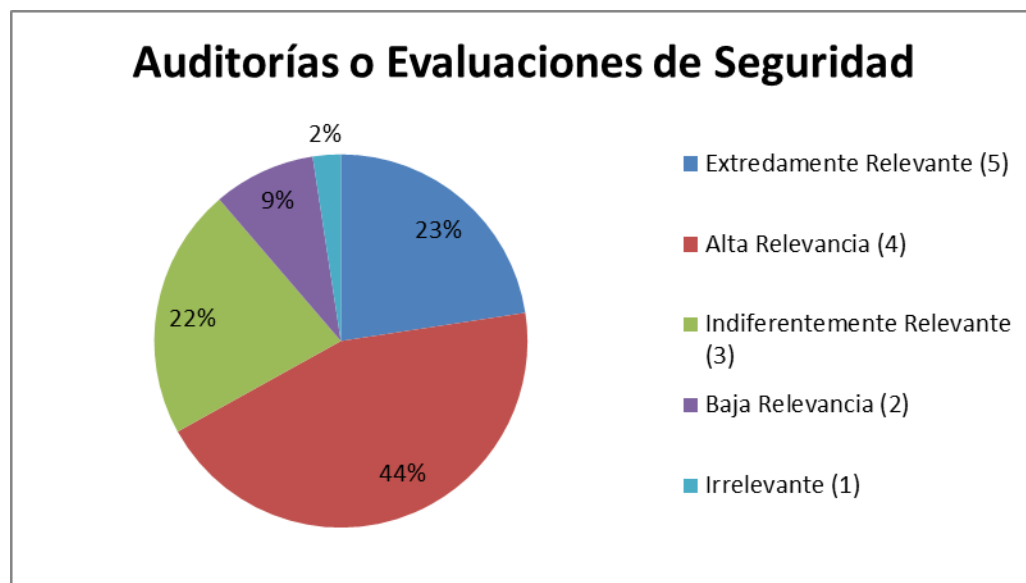
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera entonces conveniente contar con la observación de tecnología dentro del catálogo de servicios en un organismo de coordinación regional, al tener **57% de relevancia** para los expertos de la región según la opinión de la muestra.

Sobre Auditorías o Evaluaciones de Seguridad

Responde a: Relevancia o no relevancia de contar con servicios de auditorías o evaluaciones de seguridad en un eventual organismo de coordinación regional.

Resultados:



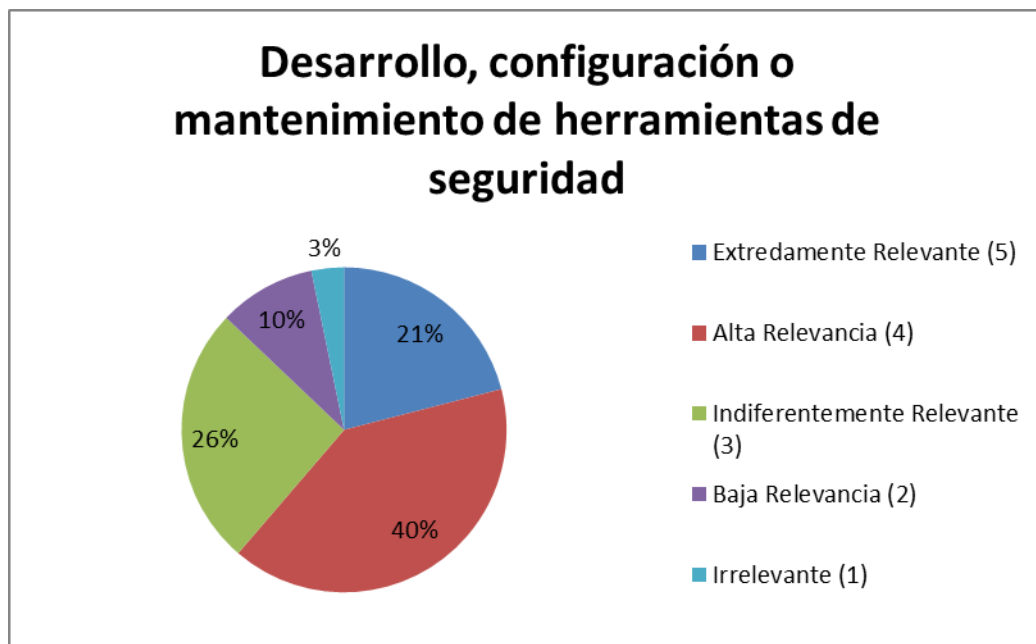
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera conveniente contar con Auditorías o Evaluaciones de Seguridad dentro del catálogo de servicios en un organismo de coordinación regional, al tener **67% de relevancia** para los expertos de la región según la opinión de la muestra.

Sobre desarrollo, configuración o mantenimiento de herramientas de seguridad

Responde a: Relevancia o no relevancia de contar con servicios de desarrollo, configuración o mantenimiento de herramientas de seguridad en un eventual organismo de coordinación regional.

Resultados:



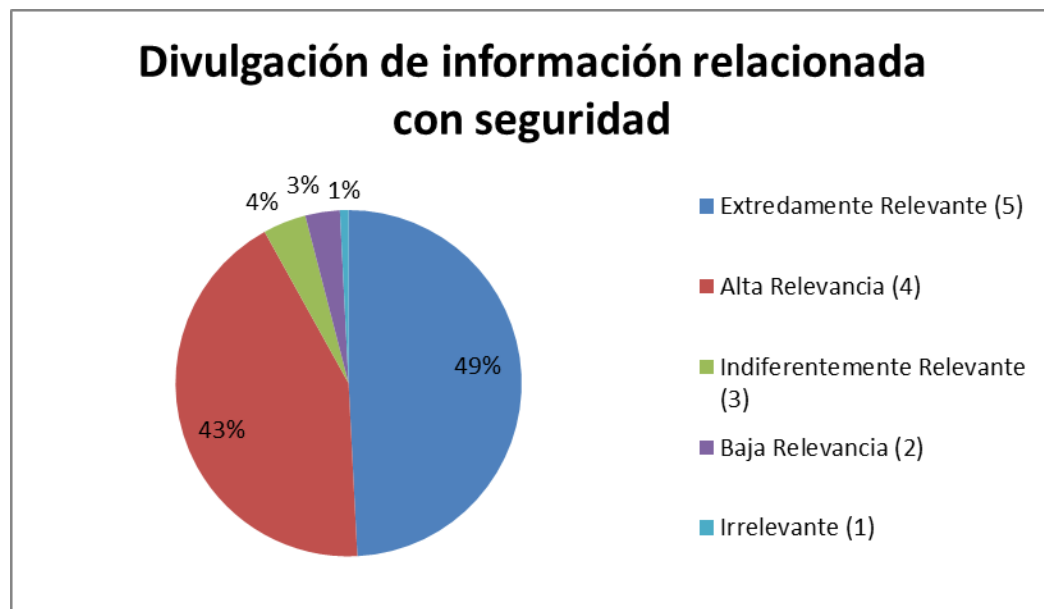
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante contar con desarrollo, configuración o mantenimiento de herramientas de seguridad dentro del catálogo de servicios en un organismo de coordinación regional, al tener **61% de relevancia** para los expertos de la región según la opinión de la muestra.

Sobre divulgación de información relacionada con seguridad

Responde a: Relevancia o no relevancia de contar con servicios de divulgación de información relacionada con seguridad en un eventual organismo de coordinación regional.

Resultados:



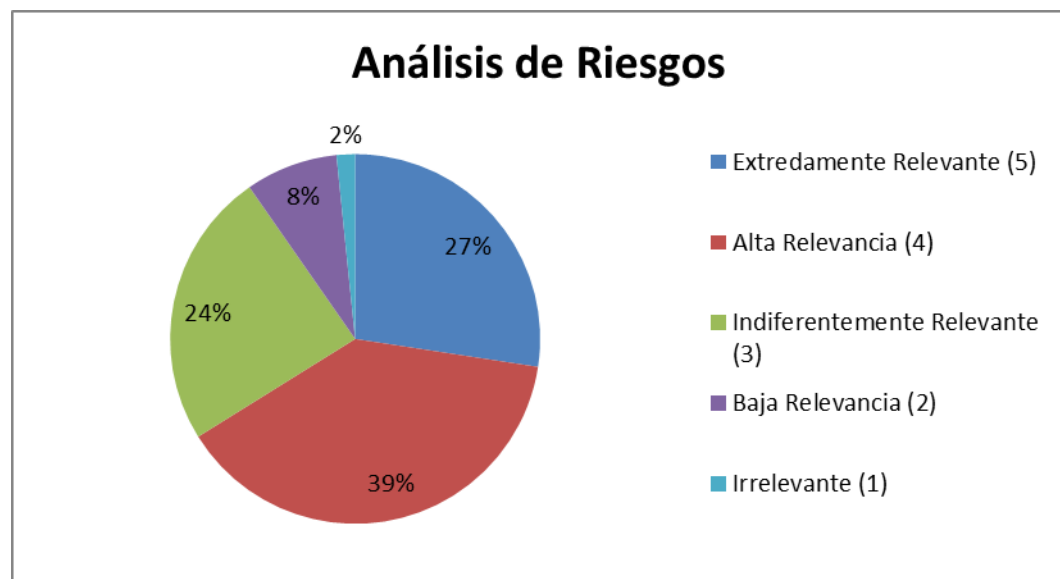
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera imprescindible contar con divulgación de información relacionada con seguridad dentro del catálogo de servicios de un organismo de coordinación regional, al tener 92% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

Sobre análisis de riesgos

Responde a: Relevancia o no relevancia de contar con servicios de análisis de riesgos en un eventual organismo de coordinación regional.

Resultados:



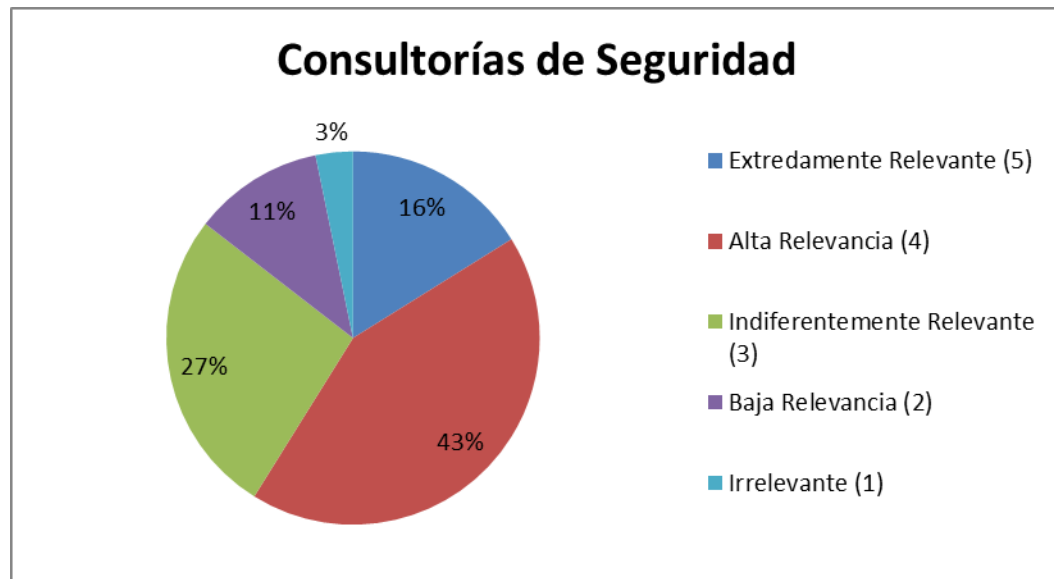
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante contar con análisis de riesgos dentro del catálogo de servicios de un organismo de coordinación regional, al tener 66% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

Sobre consultorías de seguridad

Responde a: Relevancia o no relevancia de contar con servicios de consultorías de seguridad en un eventual organismo de coordinación regional.

Resultados:



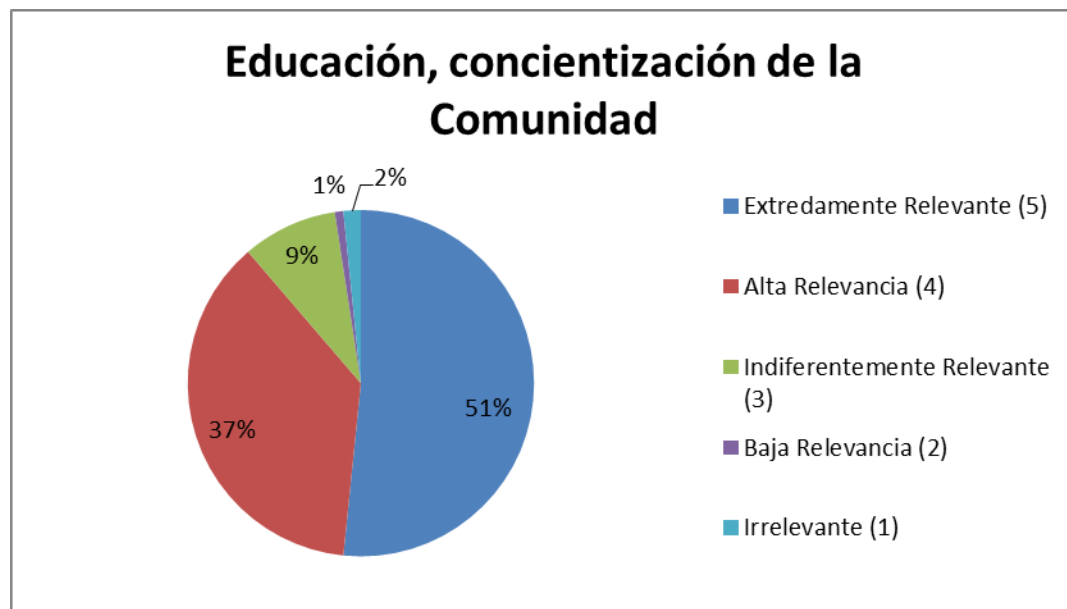
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante contar con consultorías de seguridad dentro del catálogo de servicios de un organismo de coordinación regional, al tener 70% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

Sobre educación y concientización de la comunidad

Responde a: Relevancia o no relevancia de contar con servicios de educación y concientización de la comunidad en un eventual organismo de coordinación regional.

Resultados:



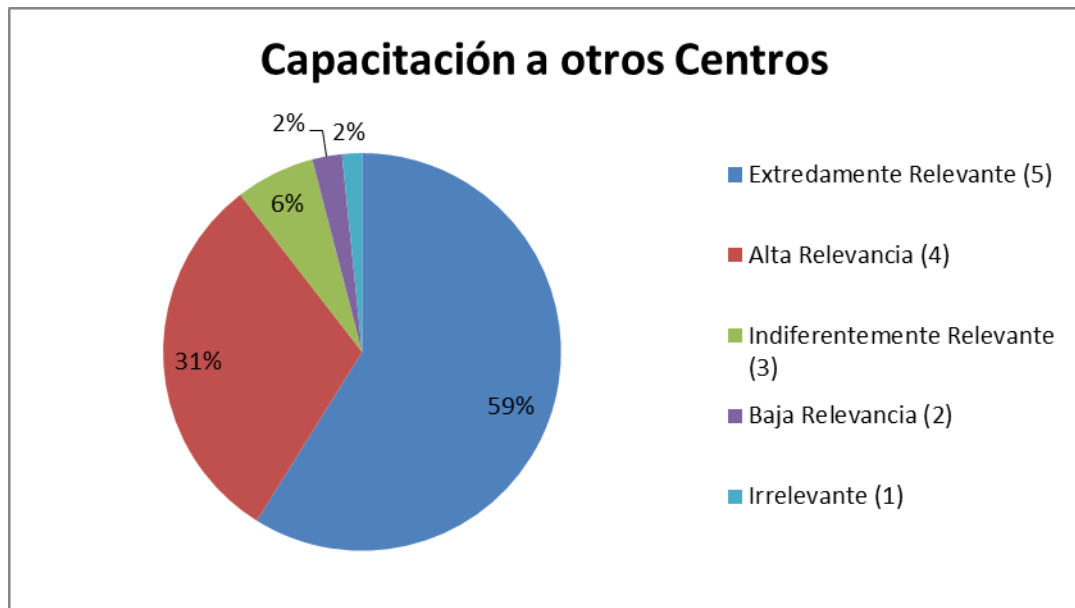
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera imprescindible contar con servicios de educación y concientización dentro del catálogo de servicios de un organismo de coordinación regional, al tener 88% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

Sobre capacitación a otros centros u organismos.

Responde a: Relevancia o no relevancia de contar con servicios de capacitación a otros centros u organismos en un eventual organismo de coordinación regional.

Resultados:



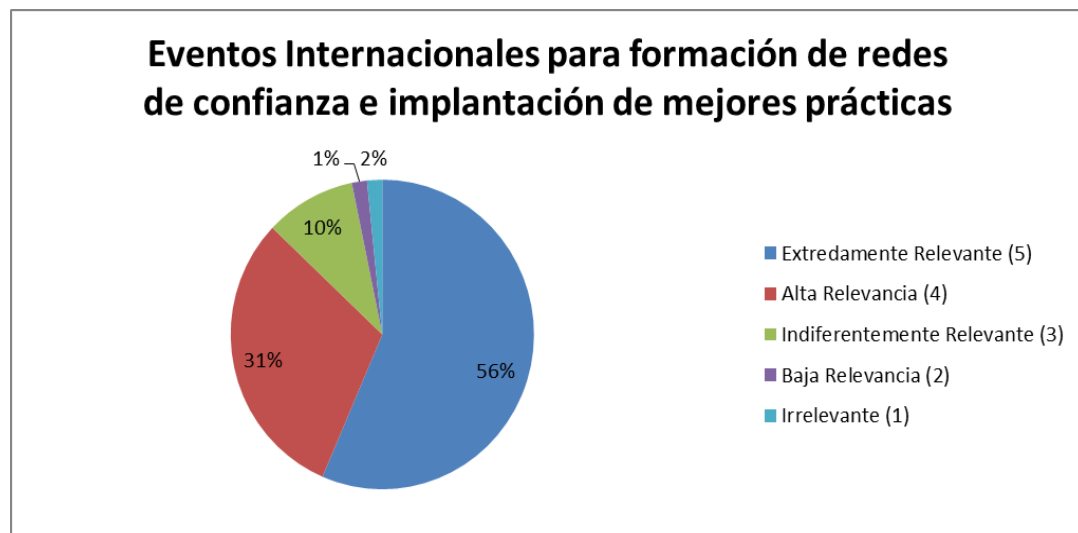
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera imprescindible contar con servicios de capacitación a otros centros u organismos dentro del catálogo de servicios de un organismo de coordinación regional, al tener 90% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

Sobre eventos internacionales para formación de redes colaborativas.

Responde a: Relevancia o no relevancia de contar con eventos internacionales para formación de redes colaborativas en un eventual organismo de coordinación regional.

Resultados:



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera imprescindible contar con eventos internacionales para formación de redes colaborativas dentro del catálogo de servicios de un organismo de coordinación regional, al tener 87% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

8.1- ANEXO I. RESUMEN DE SERVICIOS MÁS VALORADOS

Se detallan a continuación aquellos servicios que han sido valorados con más de un 80%, en los tópicos extremada/alta relevancia.

SERVICIO	VALORACIÓN
Divulgación de Información relacionada con Seguridad	92%
Coordinación para la respuesta a incidentes de seguridad	90%
Capacitación a otros Centros de Respuesta	90%
Educación, concientización de la Comunidad	88%
Realización de Eventos Internacionales de Seguridad	87%
Alertas y advertencias	82%

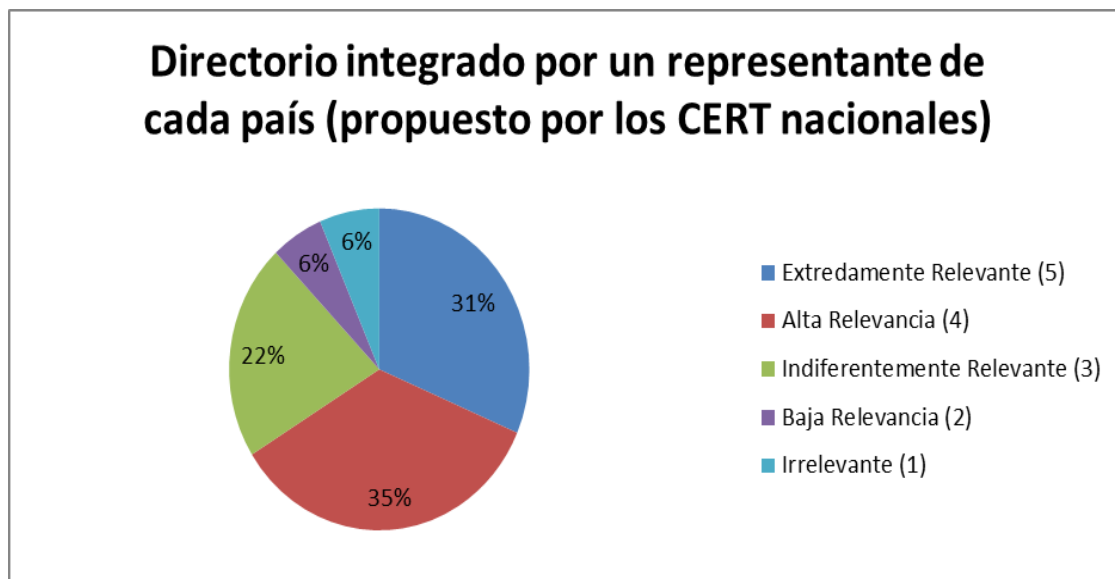
ANÁLISIS DE RESULTADOS

“GOBERNABILIDAD Y EJECUCIÓN”

Sobre la integración del Directorio

Responde a: Relevancia o no relevancia de contar un directorio integrado por un representante de cada país en un eventual organismo de coordinación regional.

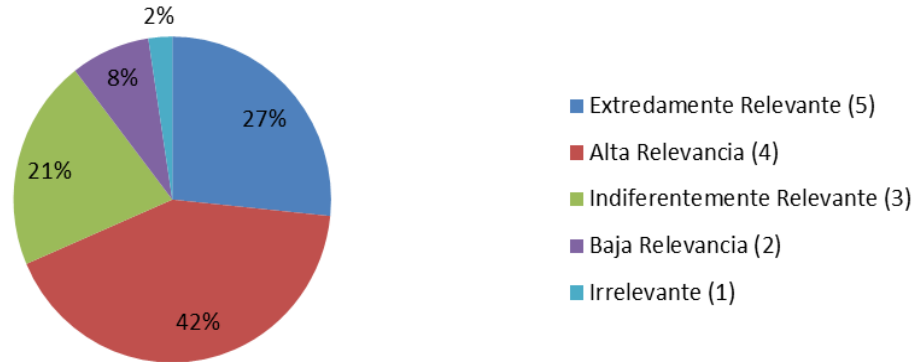
Resultados:



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante contar con un directorio integrado por un representante de cada país en la estructura de un organismo regional de coordinación, al tener 66% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

Directorio integrado por un representante de cada CSIRT (propuesto por los CSIRT's integrantes de la red)



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera también relevante la posibilidad de que el directorio se encuentre integrado por un representante de cada CSIRT al tener 69% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

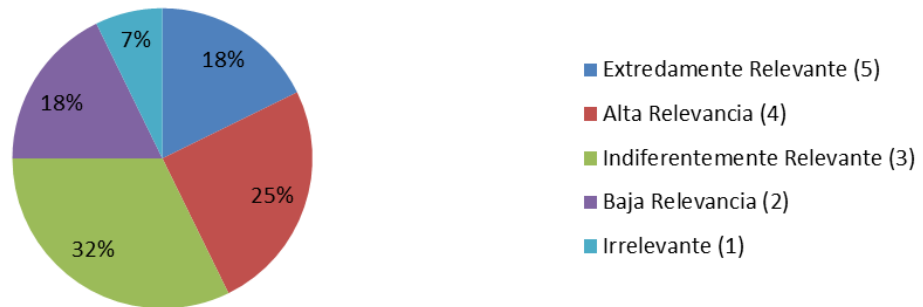
Directorio integrado por personas destacadas en la región, con actividades demostradas en gestión de incidentes



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante la integración de personas con un nivel de experiencia considerable al tener 69% que engloba altos grados de relevancia para los expertos de la región según la opinión de la muestra.

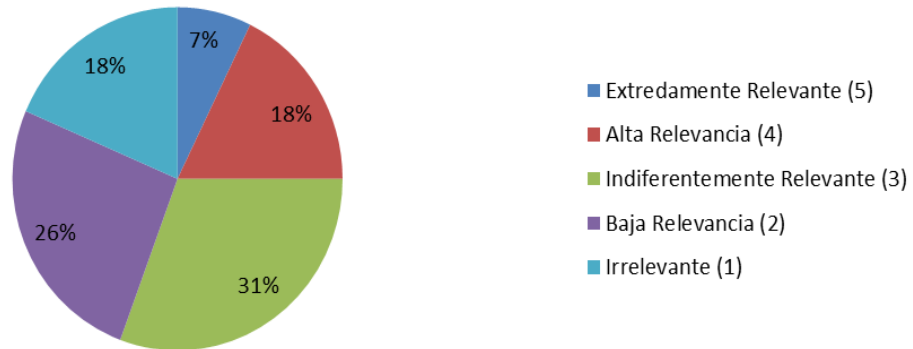
Directorio académico designado por las Universidades de la región, que tengan vinculación con Seguridad Informática



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera no denota relevancia considerable en que el directorio sea designado por las universidades de la región, sin embargo, es importante la presencia académica, lo cual se refleja en algunas opiniones en un 42% de importancia.

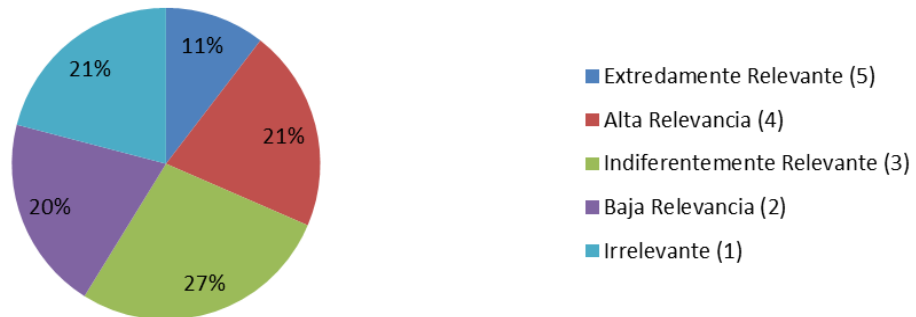
Directorio de 5 representantes, designados por asamblea representativa proporcional



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, utilizar como mecanismo de organización una estructura que sea elegida por una asamblea representativa no es considerada de relevancia ya que se demuestra una baja percepción por parte de la muestra, pues solamente un 36% de los expertos de la región creen pertinente ese tipo de designación.

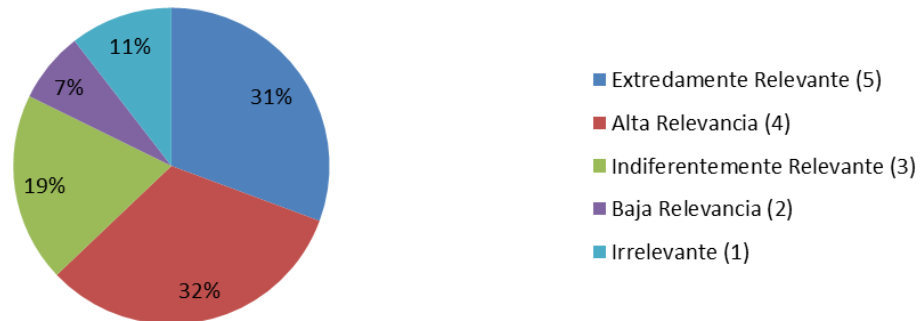
Directorio de 5 representantes, elegido por la comunidad, por voto directo electrónico



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera que utilizar el voto electrónico no generaría gran relevancia ya que se demuestra una baja percepción por parte de la muestra, pues solamente un 32% de los expertos de la región creen pertinente ese tipo de mecanismo.

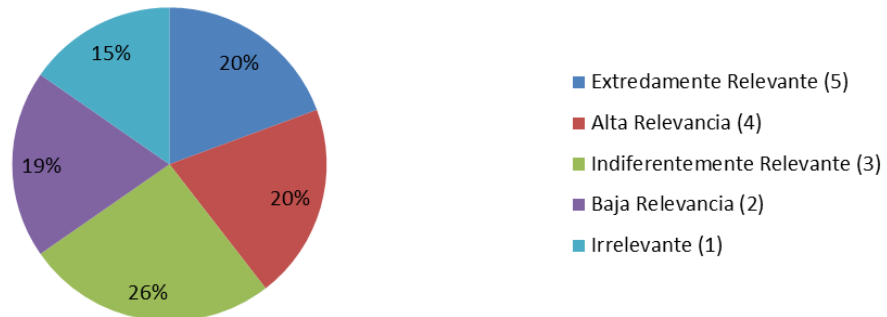
El Directorio debe ser renovado cada 2 años, en forma alternada (2 y 3)



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la renovación de ciclos de 2 años debe ser tomada en consideración y relevancia para la gestión de un organismo regional de coordinación, se demuestra que un 63% de la muestra lo considera dentro de altos grados de relevancia.

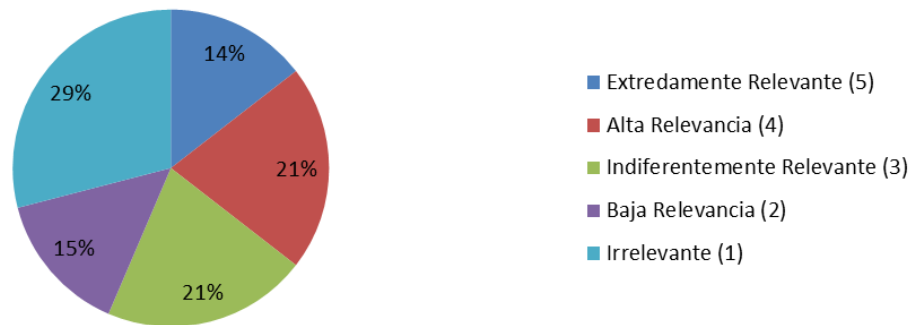
El Directorio debe ser renovado cada 4 años, en forma alternada (2 y 3)



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera que la renovación de ciclos de 4 años no es vista como una opción de relevancia para la gestión del directorio, se demuestra que un 60% de la muestra no lo considera dentro de altos grados de relevancia.

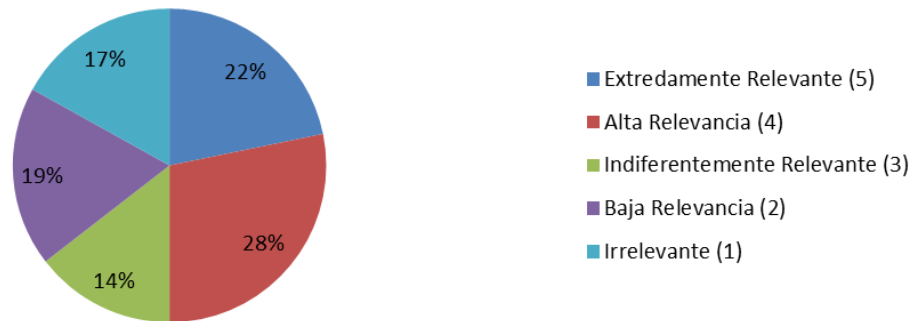
Se puede re-elegir a los candidatos al Directorio indefinidamente



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera que la posibilidad de re-elegir a los integrantes del directorio indefinidamente no es considerada una buena práctica en la gestión del directorio, al demostrarse que un 65% de la muestra no lo considera dentro de altos grados de relevancia.

Se puede re-elegir a los candidatos al Directorio sólo por una vez



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, se denota una opinión dividida de la población encuestada, al tener un 50% de la que considera de altos grados de relevancia una re-elegir a los candidatos sólo por una vez. El otro 50% no lo considera relevante.



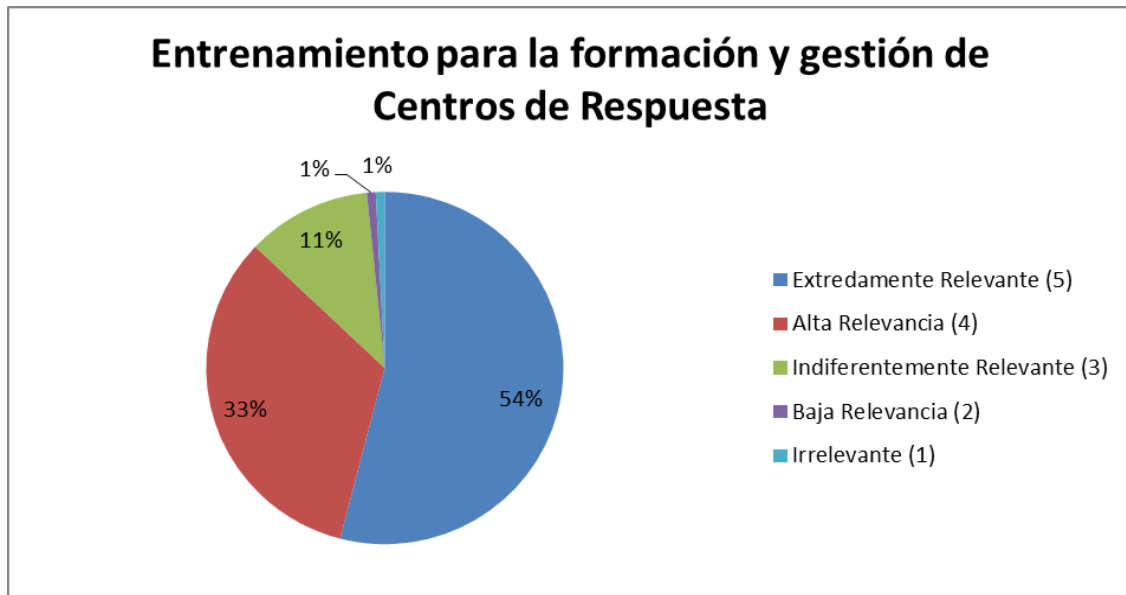
8.2.- ANEXO I. RESUMEN DE OPINIONES DE GOBERNABILIDAD

Se detallan a continuación los resultados de las consultas

SERVICIO	VALORACIÓN
Directorio por un repres. de cada país	63%
Directorio por un repres. x Csirt	69%
Directorio por personas destacadas de la región	69%
Directorio Académico	42%
Directorio elegido por asamblea representativa	36%
Directorio elegido por voto electrónico	32%

ANALISIS DE RESULTADOS

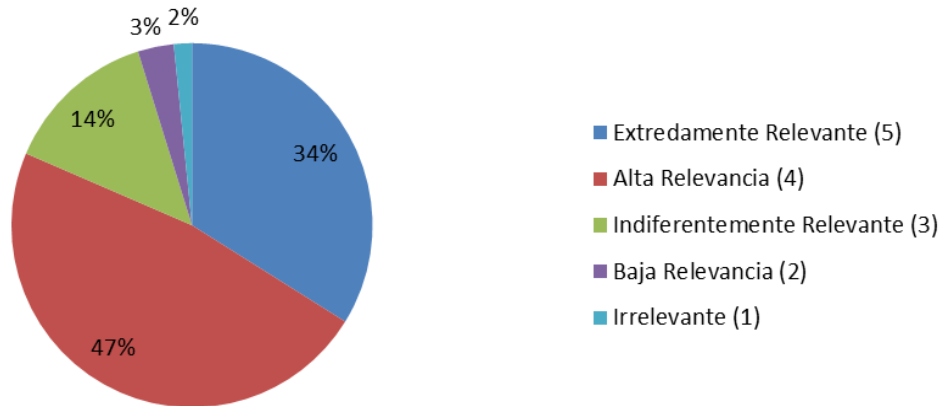
“ENTRENAMIENTO Y CAPACITACION”



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, se puede concluir que establecer una red de entrenamiento para la formación y gestión es visualizado por la población encuestada como un factor indispensable dentro de la extensión que debería tener un organismo de coordinación regional. Esto es demuestra con un 87% de la opinión de la muestra.

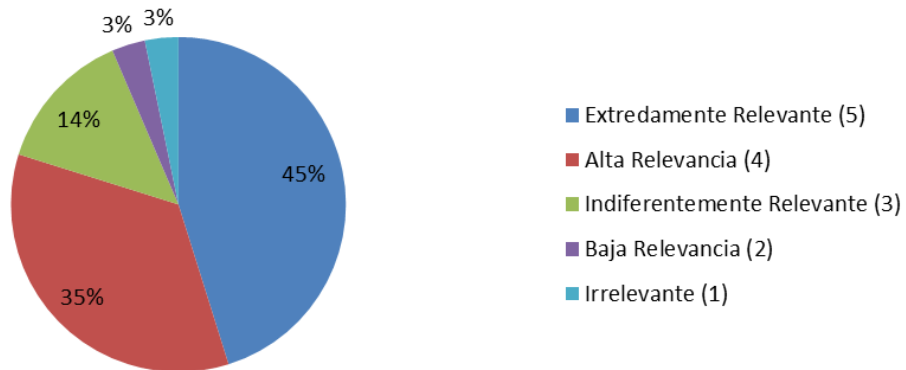
Entrenamiento para el gerenciamiento de Centros de Respuesta



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, se demuestra que es vital el entrenamiento para el gerenciamiento para liderar un organismo de coordinación al presentar la muestra un 81% de altos grados de relevancia para la población encuestada.

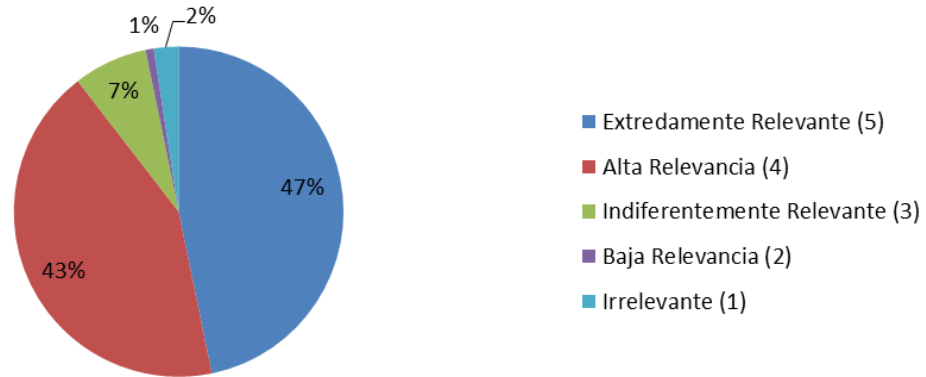
Entrenamiento en el uso de herramientas forenses



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

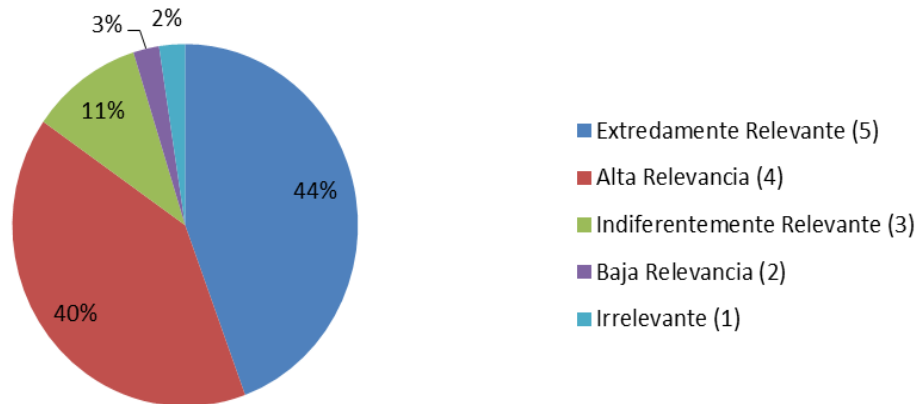
Por lo anterior, se concluye que debe existir formación técnica para el uso de herramientas forenses en función de poseer personal preparado y calificado dentro de un organismo de coordinación regional, esto se ve reflejado en la opinión de un 80% de altos grados de relevancia de la población encuestada.

Talleres de resolución de incidentes en tiempo real (botnet)



Por lo anterior, el planteamiento de realizar talleres de “botnet” en tiempo real dentro de las labores de un organismo de coordinación regional es bien visto por la opinión de la muestra al tener 90% de altos grados de relevancia, muy probablemente también se denota la debida sensibilidad ante uno de los ataques que han provocado mayor impacto en los últimos años.

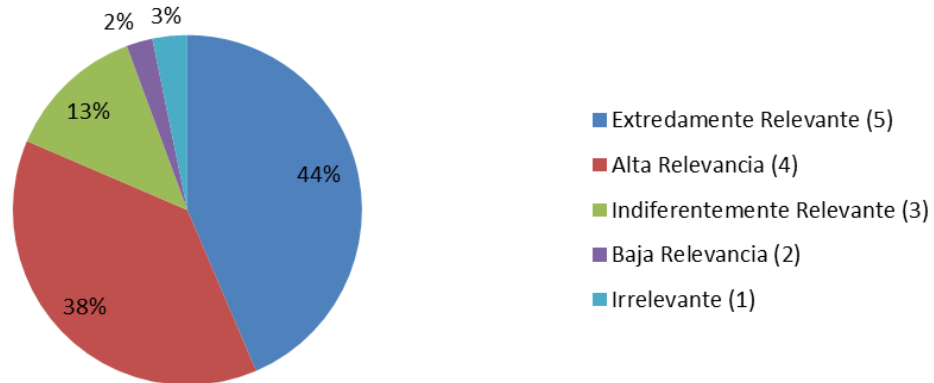
Talleres de resolución de incidentes en tiempo real (phishing)



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

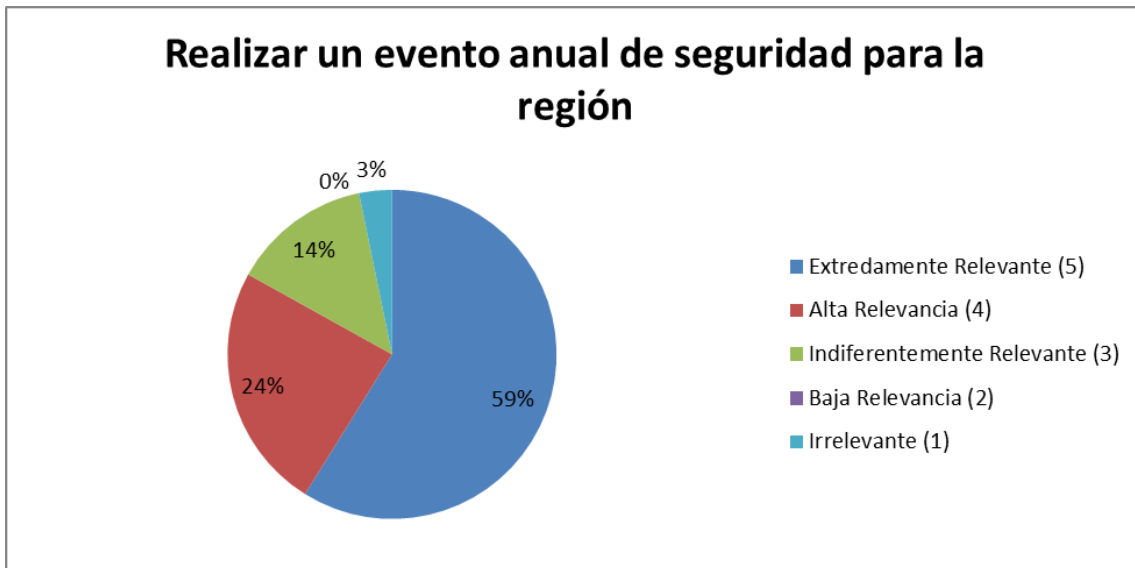
Por lo anterior, el planteamiento de realizar talleres de “phishing” en tiempo real dentro de las labores de un organismo de coordinación regional es bien visto por la opinión de la muestra al tener 84% de altos grados de relevancia.

Talleres de resolución de incidentes en tiempo real (honeynet)



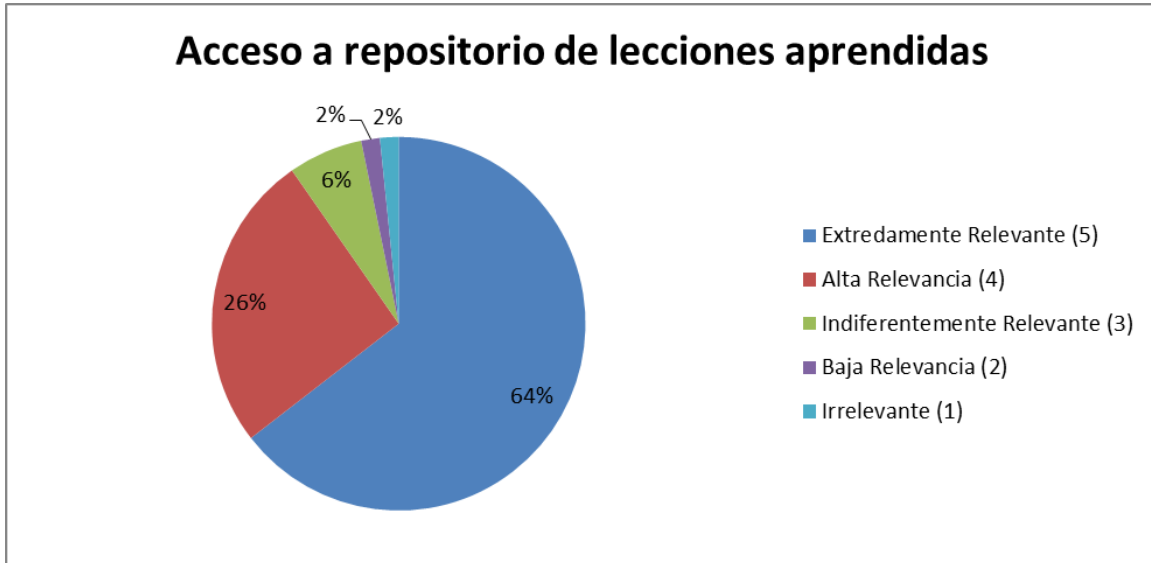
Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, el planteamiento de realizar talleres de “honeynet” en tiempo real dentro de las labores de un organismo de coordinación regional es bien visto por la opinión de la muestra al tener 82% de altos grados de relevancia.



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera que prever la realización de un evento anual de seguridad como extensión y divulgación de la temática de seguridad en la región es relevante. La opinión de la muestra lo resalta con 83% de altos grados de relevancia.



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera que el acceso a bases de datos de conocimiento se perfila con altos grados de relevancia que debe ofrecer un organismo de coordinación regional. La opinión lo destaca con un 90%.

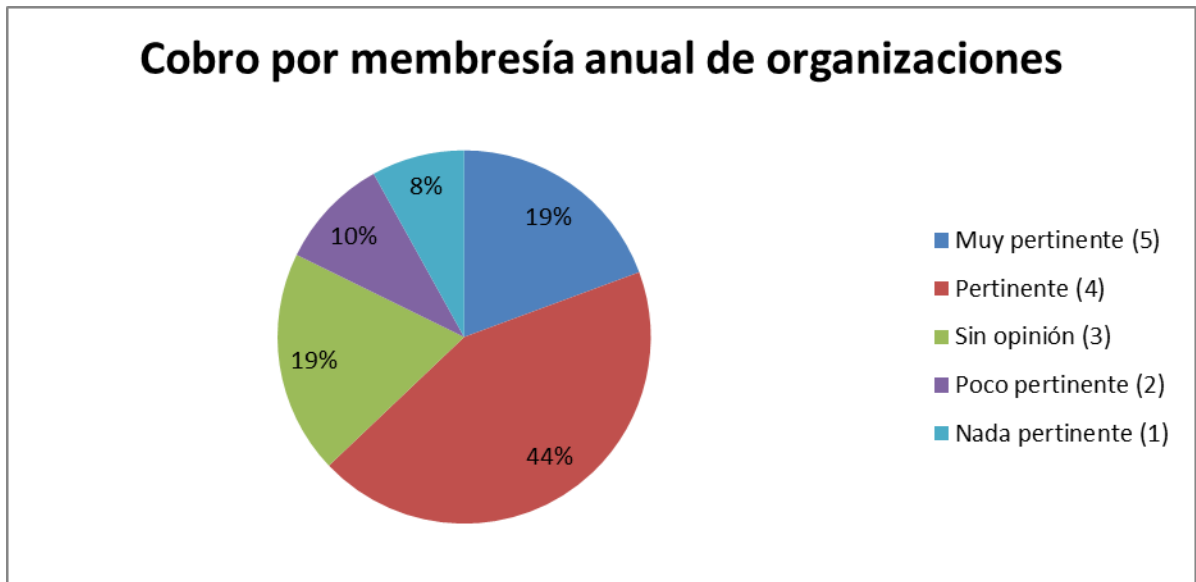
8.3.- ANEXO I. RESUMEN DE ENTRENAMIENTO Y CAPACITACIÓN

Se detallan a continuación los resultados de las consultas

TIPO DE ENTRENAMIENTO	VALORACIÓN
Formación y gestión de Centros de Respuesta	87%
Gerenciamiento de Centros de Respuesta	81%
Uso de herramientas forenses	80%
Resolución de incidentes en tiempo real (botnet)	90%
Resolución de incidentes en tiempo real (phishing)	84%
Resolución de incidentes en tiempo real (honeynet)	82%
Realizar un evento anual de seguridad para la región	83%
Acceso a repositorio de lecciones aprendidas	90%

ANALISIS DE RESULTADOS

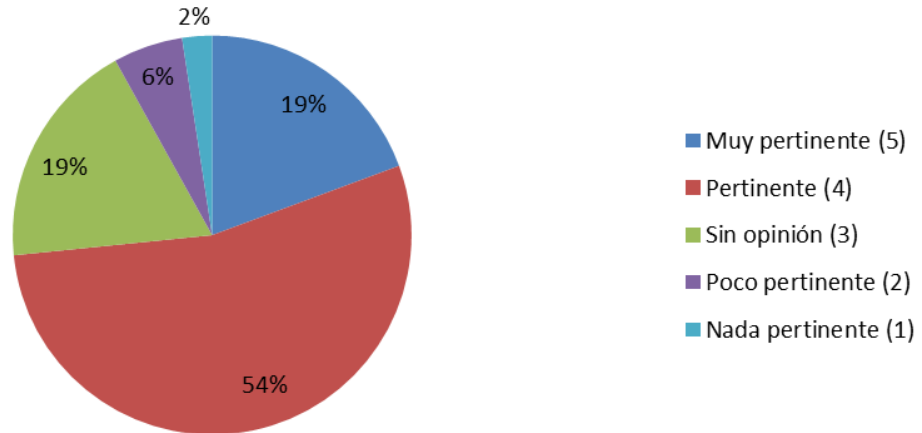
“FINANCIAMIENTO”



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 63% de altos grados, que eventualmente el financiamiento de un organismo coordinador se sustente por membresía anual de organizaciones.

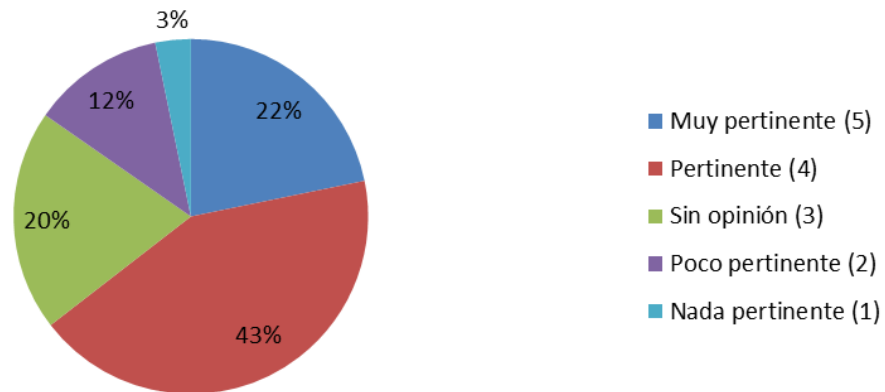
Cobros por entrenamientos y capacitación



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 73% de altos grados, que eventualmente el financiamiento de un organismo coordinador se sustente con cobros por entrenamientos y capacitación.

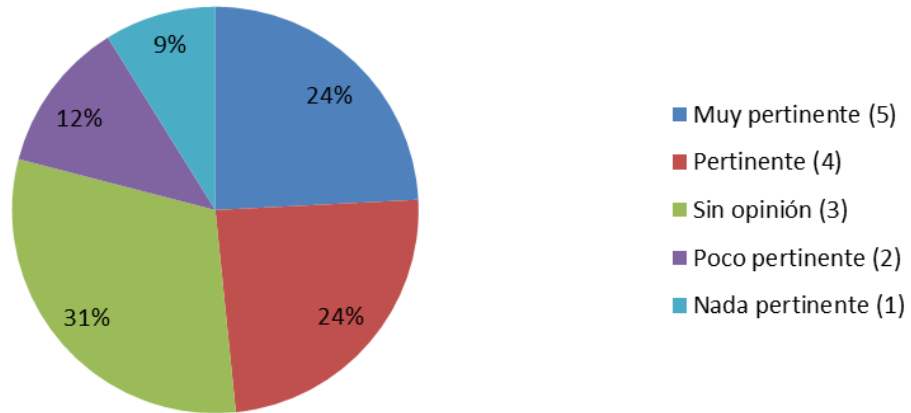
Financiamiento por parte de una organización que hospede el proyecto



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 65% de altos grados, que eventualmente el financiamiento de un organismo coordinador sea sustentando por la organización que hospede el proyecto.

Préstamos de organismos internacionales



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

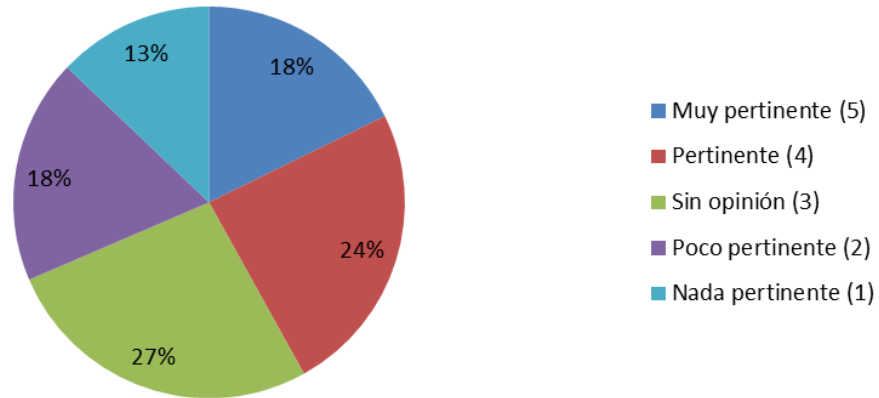
Por lo anterior, la población encuestada no considera pertinente en un 48%, que eventualmente el financiamiento de un organismo coordinador sea sustentando por préstamos de organismos internacionales.



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 67% de altos grados, que eventualmente el financiamiento de un organismo coordinador sea sustentando cobros por consultorías

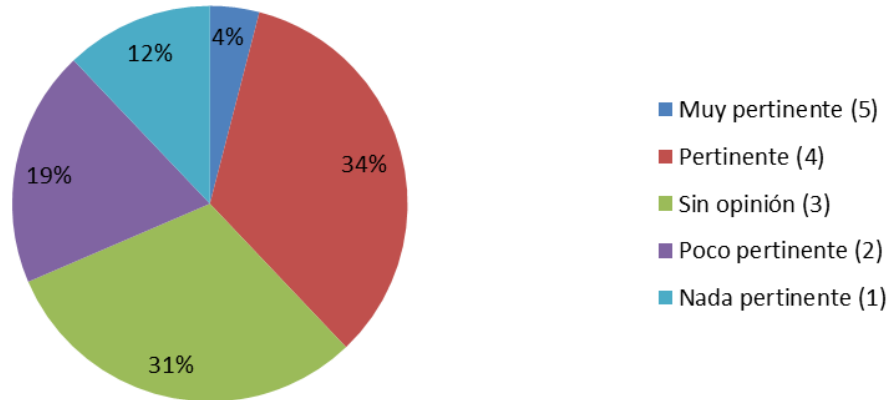
Cobros por asesoramiento en incidentes



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 51% de altos grados, que eventualmente el financiamiento de un organismo coordinador sea sustentando por cobros de asesoramientos en incidentes, por otro lado, se denota parte de la opinión que no cree pertinente ese tipo de prácticas, esto con un 49% de la misma.

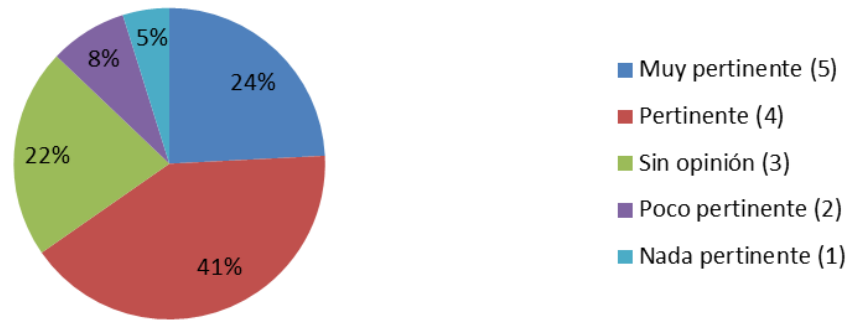
Cobros por membresía anual de personas



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada no considera relevante con un 62%, que eventualmente el financiamiento de un organismo coordinador sea sustentando por membresías anuales de personas.

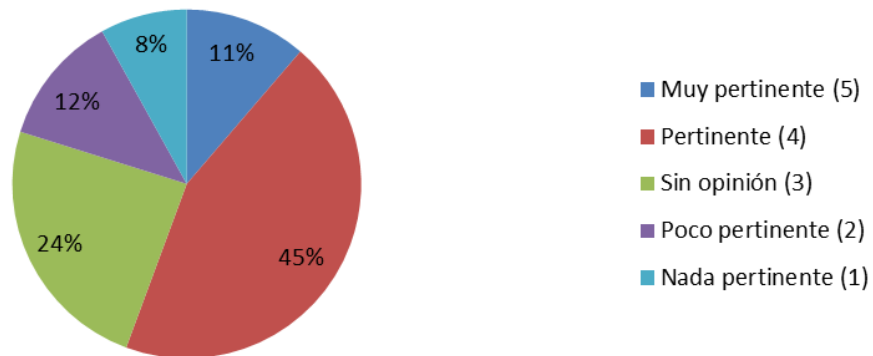
Cobros por certificaciones de sistemas de seguridad de la información



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 65% de altos grados, que eventualmente el financiamiento de un organismo coordinador sea sustentando cobros de certificaciones de seguridad de la información.

Cobros por mantenimiento de certificaciones personales de gestión de incidentes



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 56% de altos grados, que eventualmente el financiamiento de un organismo coordinador sea sustentando por mantenimiento de certificaciones personales de gestión de incidentes.

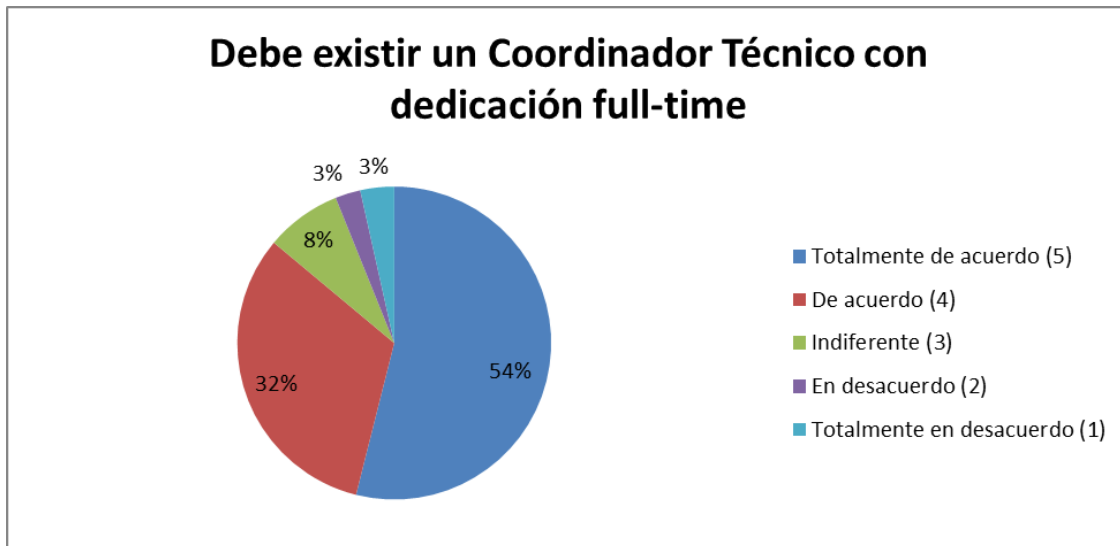
RESUMEN DE TIPOS DE FINANCIAMIENTO

Se detallan a continuación los resultados de las consultas

TIPO DE FINANCIAMIENTO	VALORACIÓN
Cobro de membresía anual a organizaciones	63%
Cobros por entrenamiento y capacitación	73%
Presupuesto por organización host	65%
Préstamo de organismos internacionales	48%
Cobros por consultoría	67%
Cobros por asesoramiento en incidentes	51%
Cobros por membresías personales	38%
Cobros por certificaciones de SGSIs	65%
Cobros por mantenimiento de certificaciones personales de gestión de incidentes	56%

ANALISIS DE RESULTADOS

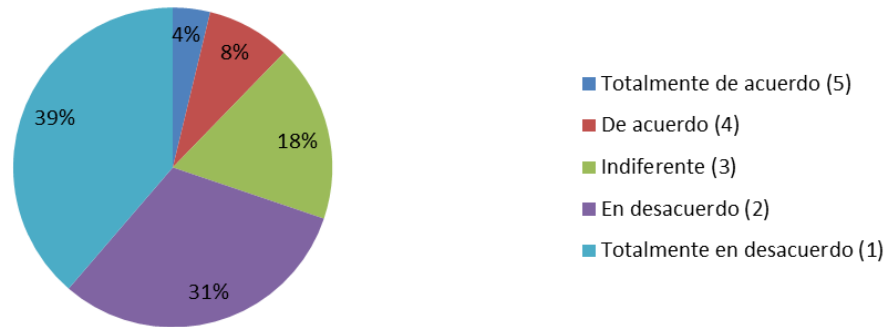
“EQUIPO TECNICO”



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

Por lo anterior, la población encuestada considera relevante con un 86% de altos grados, que eventualmente debe existir un coordinador técnico con dedicación full-time en la gestión del área en cuestión.

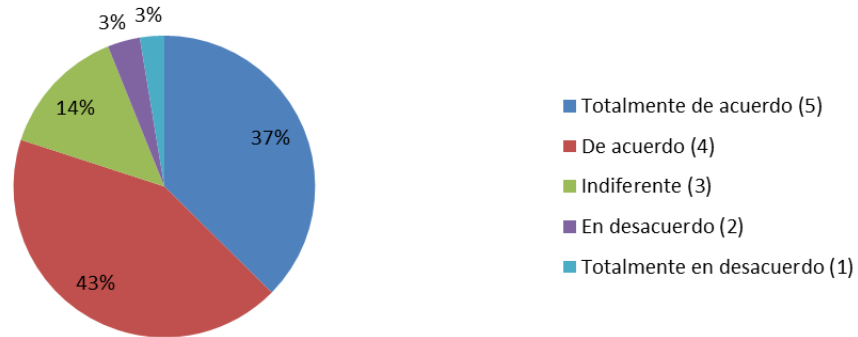
No debe existir un Coordinador Técnico, basta con coordinación horizontal entre técnicos



Fuente: Encuesta en línea de elaboración propia. Anexo N°1

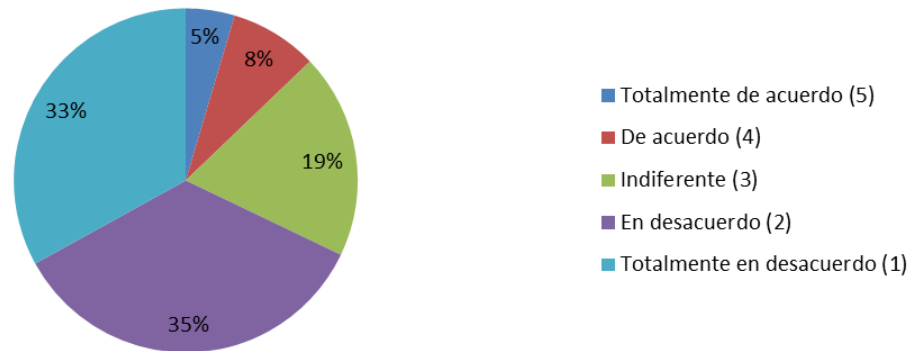
Por lo anterior, la población encuestada considera relevante con un 70% que exista una coordinación horizontal entre técnicos y que no se refleje solamente en un rol indicado.

Los técnicos pueden estar alocados en diferentes países y reportar al Coordinador Técnico



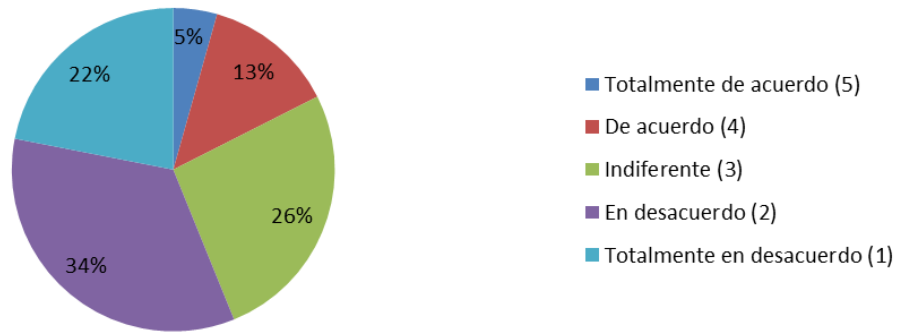
Por lo anterior, la población encuestada considera relevante con un 80% que los técnicos estén alocados en diferentes países y reportar al coordinador técnico según corresponda.

Basta con un Coordinador Técnico con dedicación part-time



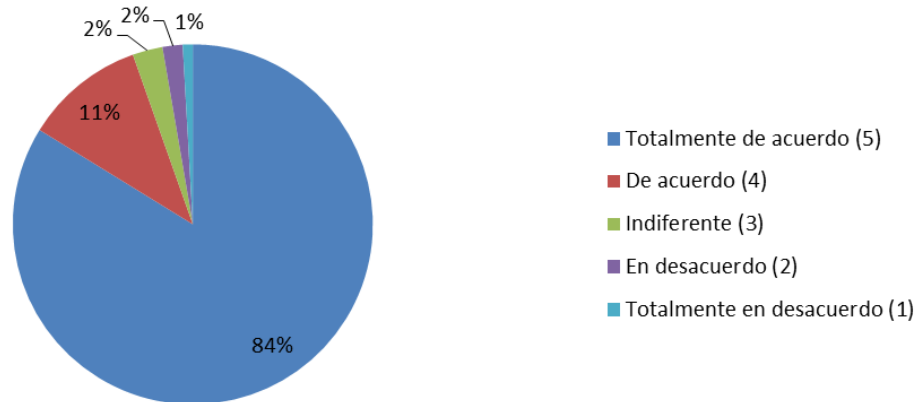
Por lo anterior, la población encuestada considera irrelevante con un 68% que exista solamente un coordinador técnico con dedicación part-time en el área correspondiente.

Los técnicos y el Coordinador Técnico tienen que estar alocados en una misma oficina



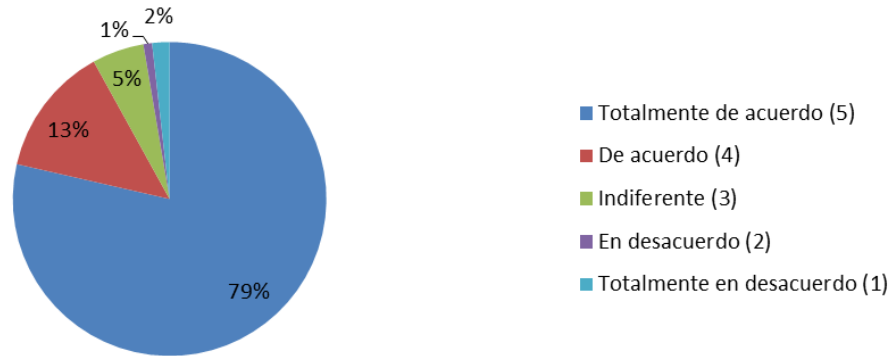
Por lo anterior, la población encuestada considera irrelevante con un 56% que los técnicos y el coordinador técnico estén localizados en una misma oficina de coordinación.

Los técnicos deben firmar el código de ética y acuerdos de confidencialidad con el centro



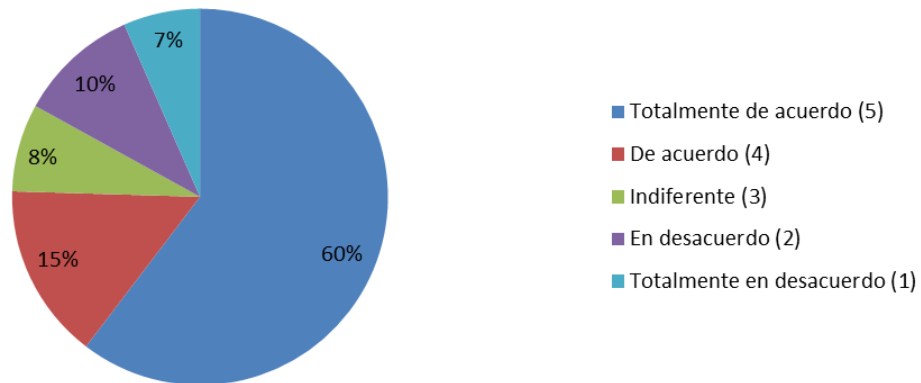
Por lo anterior, la población encuestada considera relevante con un 95% que los técnicos deben firmar el código de ética y acuerdos de confidencialidad con el organismo de coordinación regional.

Los técnicos deben tener una red de comunicaciones segura



Por lo anterior, la población encuestada considera relevante con un 92% que debe existir una red segura y la infraestructura necesaria para tener comunicaciones seguras.

Los técnicos no deben emitir comunicados públicos sobre ningún incidente



Por lo anterior, la población encuestada considera relevante con un 75% que la relación con comunicados públicos no deben ser emitidos por técnicos del organismo de coordinación.

8.5.- ANEXO I. Sobre la conformación del Equipo Técnico

Se detallan a continuación los resultados de las consultas

CONFORMACIÓN EQUIPO TÉCNICO	VALORACIÓN
Necesidad de coordinador técnico full time	86%
Los técnicos pueden estar alocados en diferentes países	80%
Debe existir un código de ética y acuerdos de confidencialidad, expresamente aceptados x los técnicos	95%
Disponer de una red de comunicaciones segura	92%

8.6.- Comentarios finales de la encuesta.

A continuación se transcriben los comentarios finales más relevantes en contenido de la encuesta realizada:

- 1- “Se entiende extremadamente importante la realización de eventos de difusión de las mejores prácticas, técnicas utilizadas por las personas que actúan en forma maliciosa y promover una red de técnicos que ayude a la rápida respuesta de los incidentes a nivel internacional.”
- 2- “Un CSIRT coordinador regional es muy importante en la actual época debido a los distintos ataques e incidentes de seguridad, en este caso los CSIRT nacionales deberían de estar previamente establecidos para mantener una comunicación y apoyo fluido.”
- 3- “Pienso que se debe considerar el tema de la vinculación de la Educación en temas de seguridad, que haya una parte para la Investigación científica en temas de seguridad informática, crear masa crítica en las Universidades por medio de llamados a proyectos de investigación para fomentar la cultura de Seguridad a nivel de toda la región debido a que no en todos los países hay en los pensum de estudios universitarios materias de seguridad.”
- 4- “El desafío más importante es definir el grado de "confianza" que va a tener el centro de respuesta en todos los países a los que formen parte. Me parece importante el papel que pueden jugar las Universidades en este punto. Espero que este proyecto llegue a buen puerto porque es algo que hace realmente falta.”
- 5- “Considero importante reflexionar sobre cual sería el status formal del Centro, más allá de contar con un órgano de dirección como lo es el mencionado directorio, de quien dependería políticamente el Centro.”
- 6- “Identificar referentes de capacitación en cada país de la región. Apuntar a brindar una carrera de grado en Seguridad Informática que podría tener un nivel común para todos los



países del área. Considerar para esta carrera la posibilidad de que sea completamente on line o virtuales.”

7- “Dar más divulgación sobre estos temas y tener un representante para que esto se haga más extensivo a nivel no solo público sino privado.”

8- “The most important question to be asked was: is there a need to a CSIRT for the region? I think there is a need for a forum for CSIRTs, but not for a coordinating CSIRT. I don't see a point in us repeting the errors of Europe when they tried to create the "EuroCERT" back in the 90's. Really, one thing is the cooperation of teams, other is a team of a country sending data to people of other countries or having external people handling sensitive data. I'm sad AMPARO is even considering the creation of an operational CSIRT for the region. This questionnaire assumes the decision of creating a team has already been taken. There is no option to say "I don't see a relevance", and there are no questions that give an option of forming a structure similar to TF-CSIRT or APCERT -- they are not operational, they are a coalision of CSIRTs that work towards cooperation.”

9- “Los CERT’s Nacionales están sujetos a las leyes locales y se deben buscar mecanismos jurídicos que les permitan compartir información con el coordinador regional.”